Refine Search

Search Results -

Terms	Documents
"one-stop shopping" and @pd<=19991230	3

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L43

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Sunday, November 07, 2004 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR			
L43	"one-stop shopping" and @pd<=19991230	3	L43
DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR			
L42	L41 and (bill$ with pay$) and (regist$ or enroll$)	2	L42
L41	6606744.pn. or 6427132.pn.	2	L41
L40	L39 and (bill$ with pay$)	3	L40
L39	L38 and (inter$ with (computer or network$))	5	L39
L38	L36 and server$	6	L38
L37	"one-stop shopping".clm. and @ad<=19991230	0	L37
L36	L35 and (internet or www or web$ or online or "on-line")	7	L36
L35	L34 and 705/26,27.ccls.	7	L35
L34	"one-stop shopping" and @ad<=19991230	46	L34
DB=PGPB,USPT; THES=ASSIGNEE; PLUR=YES; OP=OR			
L33	L32 and (reduc$ with fluctuat$)	5	L33

L40: Entry 2 of 3 File: USPT Jul 30, 2002

US-PAT-NO: 6427132
DOCUMENT-IDENTIFIER: US 6427132 B1

TITLE: System, method and article of manufacture for demonstrating E-commerce capabilities via a simulation on a network

DATE-ISSUED: July 30, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Bowman-Amuah; Michel K.	Colorado Springs	CO		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Accenture LLP	Palo Alto	CA			02

APPL-NO: 09/ 388028 [PALM]
DATE FILED: August 31, 1999

INT-CL: [07] G06 F 9/45, G06 G 7/48

US-CL-ISSUED: 703/22; 703/6, 705/26
US-CL-CURRENT: 703/22; 703/6, 705/26

FIELD-OF-SEARCH: 703/1, 703/2, 703/6, 703/13, 703/22-23, 705/26, 705/27, 705/39

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5295244	March 1994	Dev et al.	395/161
☐	5461611	October 1995	Drake, Jr. et al.	370/54
☐	5652787	July 1997	O'Kelly	379/112
☐	5694548	December 1997	Baugher et al.	395/200
☐	5864823	January 1999	Levitan	105/14
☐	5944795	August 1999	Civanlar	709/227
☐	6026376	February 2000	Kenney	705/27
☐	6052670	April 2000	Johnson	705/27

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0941010	September 1999	EP	
0944209	September 1999	EP	
WO 98/18237	April 1998	WO	
WO 99/34587	July 1999	WO	

OTHER PUBLICATIONS

Parker et al, "An Internet-Mediated Business Simulation: Developing and Using TRECS", Simulation & Gaming, vol. 30, No. 1, pp. 51-69, Mar. 1999.*
Zack, "An MIS Course Integrating Information Technology and Organization Issues", Databae for Advances in Information Systems, pp. 73-87 (Spring 1998).*
Paul et al., "Simulation of Business Processes", American Behavioral Scientist, pp. 1551-1576, Aug. 1999.*
Maren S. Leizaola, Tuning IP Performance: The Right Tools for the Task, May 1998 URL: http://data.com./tutorials/tuning.html, Viewed Oct. 15, 1999.
Mick Seaman et al., Going the Distance with QOS, Feb. 1999, URL, http://data.com/issue/990207/distancr.hmtl, Viewed Oct. 15, 1999.
Stephen Saunders, The Policy Maker, May 1999, URL, http://data.com/issue/990507/policy.html, Viewed Oct. 15, 1999.
Dilger, "Front to Back", Manufacturing Systems, vol. 16, Issue 9, pp. 55-68 (downloaded text) (Sep. 1998).

ART-UNIT: 2123

PRIMARY-EXAMINER: Teska; Kevin J.

ASSISTANT-EXAMINER: Broda; Samuel

ATTY-AGENT-FIRM: Burton; Daphne L. Oppenheimer Wolff & Donnelly LLP

ABSTRACT:

A system, method and article of manufacture are provided for demonstrating e-commerce capabilities on a network via a simulation. Data connectivity is provided over a network between a simulated user, a simulated product distributor, a simulated product vendor, and a simulated financial service provider. An electronic catalog is displayed over a network that shows a product for sale by the simulated product vendor. The simulated user is shown browsing the electronic catalog on the network. Further, a consultation over the network, relating to the product for sale shown in the electronic catalog, is depicted between the simulated user and the simulated product distributor. Selection of the product by the simulated user is illustrated. The simulated user is portrayed to authorize payment alter an on-line review of an account of the user.

18 Claims, 110 Drawing figures

Previous Doc Next Doc Go to Doc#

L42: Entry 2 of 2 File: USPT Jul 30, 2002

DOCUMENT-IDENTIFIER: US 6427132 B1
TITLE: System, method and article of manufacture for demonstrating E-commerce capabilities via a simulation on a network

Detailed Description Text (100):
While there are components in the NGN that ensure interoperability between "NGN" and PSTN, there are also a huge new set of new services that are built entirely on the NGN components which is provide feature rich multimedia (voice, video, data) based communication services as well as enabling many eCommerce services enabled by IP technologies. These components (described later in detail) include directories, policies, user authentication, registration, and encryption. These components enable services like integrated messaging, multimedia conversations, on-demand multi-point conference, enhanced security & authentication, various classes of media transport services, numerous automations in electronic Internet commerce activities e.g. banking, shopping, customer care, education, etc. As the NGN matures third party value added service providers will develop IP based services that will combine applications such as electronic commerce (procurement, warehousing, distribution and fulfillment) as well as online banking to present the consumer with an integrated boundless shopping experience.

Detailed Description Text (106):
Given the huge revenues and global nature of PSTN services, as well as their use of SS7 and AIN technologies, components that allow interoperability between "NGN" and PSTN will need to be developed. These will include IP/PSTN Gateways, IP/PSTN address translators, IP/SS7 Gateways, IP enabled SSP's, and IP based Intelligent Peripherals. In addition to IN enablers, new components (as will be describe later) with features like directories, policies, user authentication, registration, session encryption, etc. will also be developed to enhance the IN capabilities. The NGN-IN enablers will provide the next level of intelligence in order to address communication over mixed media types, control of multiple session characteristics, collaborative communications needs, ubiquitous network access, "any to any" communications, and multimedia delivered information services. Note that these "NGN" components will continue to evolve to provide similar and enhanced capabilities in the "New Core".

Detailed Description Text (110):
Example: Assuming a US based NGN service user was roaming in Europe and wanted to access the network but has the use of specific calling information stored in his profile database in the US, how would such a challenge be overcome without replicating the user's data onto every rules database on the NGN to ensure that the user would not be denied access to features and services which the user typically subscribed. Obviously, storing or replicating this data and then managing synchronicity over a worldwide network would be process intensive, costly and cumbersome. This intelligent network architecture addresses these issues efficiently with mechanisms that make remote data available locally for the duration of a session and then caches the information in short term non-volatile memory not in the foreign rules database server. In other words although a user's profile may be physically stored in a Rules database in the United States, the user

may access the network from Europe and be automatically granted access to the specific services and features that normally would be available during his US service experience. The remote session controller in Europe would communicate with the cross network location register and rules database server to identify the subscriber's "home" rules database in order to collect the policies and profile of the subscriber for use in Europe; this is done by using the inter device message sets (command and control) over the control plane sub network. Unlike other mechanisms often employed, this mechanism does not replicate this information onto the local (European) rules database, making long term control data management predictable. The design is CORBA compliant and therefore can be interconnected with other standards based networks.

Detailed Description Text (118):
This process or application is critical since it is the "glue" between the end user application and the communications network. It is responsible for collection and distribution of end-user session preferences, application requirements, access device capability and accounting policy information to the required "IN enabling" components. In summary its main functions are to: Create the AMA/CDR and other usage records Interfaces external 3.sup.rd party Network Gateways. Liase with Clearing Houses and Cross Network Location Registers Feeds the Financial Infrastructure

Detailed Description Text (119):
Cross Network (Roaming) Location Register (Policy Management)

Detailed Description Text (120):
Similar to the Home location register in the wireless/cellular telephony world. This functional component provides the required policies governing users who access third party networks and cross geographical boundaries. It keeps in constant contact with other cross network location registers of the geographically dispersed but inter-connected networks, exchanging accounting, service feature profile and control data for local and roaming subscribers.

Detailed Description Text (168):
FIG. 1H-1 is a flowchart illustrating an Invoice and Collections Process in accordance with a preferred embodiment. First, in step 192, customer account inquiries and customer payment information is received by the system. Next, in step 193, billing data, including discounts due to quality of service violations and rebates due to service level agreement violations, is collected and processed. Thereafter, in step 194, customer account invoices are created for distribution based on the customer payment information and the billing data.

Detailed Description Text (378):
The Internet access software accesses and "handshakes" with an "Internet Entry Server", which verifies the PIN number, provides the access and times the user's access time. The Internet Entry Server is programmed to recognize the PIN number as entitling the user to a limited prepaid or "free" Internet access time for on-line help services. Such a time period could be for a total time period such as 1 hour or more, or access to on-line help services can be unlimited for 90 days, 6 months, etc., for example, with the access time paid for by the sponsor/vendor. The first time a customer uses the on-line help service, the Internet Entry Server performs a registration process which includes a number of personal questions and custom data gathering in the form of queries provided by the sponsor/vendor for response by the user.

Detailed Description Text (387):
In a lookup step 1908, the telephonic communication over the hybrid network is limited bases on a user profile. Preferably the user profile is included in a rules database. By locating the user profile within the rules database, the rules database can provide seamless cross-location registration without the need for

duplicate databases located on different networks. Using a rules database, a user utilizing the Internet in Europe can get the same telephony service as provided in the United States, as described above. Preferably the computer used to interface with the Internet includes multimedia equipment such as speakers and a microphone. Utilizing a multimedia equipped computer allows a user to use telephonic communication with little or no disruption while interfacing with the Internet. Multimedia computer speakers are used to receive the telephony audio from the network and the microphone is used to transmit the telephony data to the network.

Detailed Description Text (741):
The MySite consumer would be shown to actually browse or sample the content prior to purchasing it IP audio and video streaming, consult with the storefront operator at the click of a button on the web site (IP video conferencing) collaborate. with a subject matter expert on the configuration of the browser to decode the purchased content (T.120 white-boarding and application sharing) Join in a phone in Q/A with the authors of the content in a foreign country (multi-point IP telephony). Review a real-time bill for the costs of the transaction (real-time billing rendered over IP-Fax to a unified messaging mailbox) and finally authorize payment after an on-line account review (Secure Internet banking). The financial services. organization would illustrate the network's ability to interface with and support third party value added service providers in a secure robust fashion.

Previous Doc Next Doc Go to Doc#

L43: Entry 1 of 3 File: EPAB Dec 12, 1996

PUB-NO: WO009639689A1
DOCUMENT-IDENTIFIER: WO 9639689 A1
TITLE: INFORMATION RETRIEVAL SYSTEM FOR DRIVERS

PUBN-DATE: December 12, 1996

INVENTOR-INFORMATION:

NAME	COUNTRY
LIEBESNEY, JOHN P	US

ASSIGNEE-INFORMATION:

NAME	COUNTRY
SMART ROUTE SYSTEMS LIMITED PA	US
LIEBESNEY JOHN P	US

APPL-NO: IB09600539
APPL-DATE: June 1, 1996

PRIORITY-DATA: US46105295A (June 5, 1995)

INT-CL (IPC): G08 G 1/0962
EUR-CL (EPC): G08G001/0962; G01C021/36

ABSTRACT:

CHG DATE=19990617 STATUS=O>A user-friendly and interactive multi-modal video/audio user information real-time service and apparatus covering substantially all important and alternative aspects of an informational area, such as travel by various modes, to provide "one-stop shopping" for a user with such integrated multi database consolidation, and with user interaction with the video screen presentations, locally or remotely, to access the same and perform intelligent branching.

L43: Entry 2 of 3 File: TDBD Dec 1, 1999

TDB-ACC-NO: NNRD428118

DISCLOSURE TITLE: Customer Premises Equipment Providing Wireless Clients Access to Consolidated Broadband Services

PUBLICATION-DATA:
IBM technical Disclosure Bulletin, December 1999, UK

ISSUE NUMBER: 428
PAGE NUMBER: 1682

PUBLICATION-DATE: December 1, 1999 (19991201)

CROSS REFERENCE: 0374-4353-0-428-1682

DISCLOSURE TEXT:

Disclosed is equipment that connects wireless devices on the customer premises to a broadband network using standard wireless protocols. A preferred embodiment uses the wireless protocols defined by the Bluetooth (TM) Special Interest Group; see www.bluetooth.com for details. The term "broadband network" includes, but is not limited to, the cable television cable plant, asymmetrical digital subscriber line (ADSL) connected to a telephone carrier's local loop, digital satellite television transmissions, and wireless bypass to a local carrier's point of presence using a broadband wireless technology such as LMDS.

L43: Entry 3 of 3 File: DWPI Dec 14, 1999

DERWENT-ACC-NO: 2000-115223
DERWENT-WEEK: 200010

TITLE: Shoppers aiding system in selection and location of articles displayed for sale in stores

INVENTOR: TALBOTT, T G; TALBOTTT, A F

PATENT-ASSIGNEE: TALBOTT T G (TALBI), TALBOTTT A F (TALBI)

PRIORITY-DATA: 1993US-0023955 (February 26, 1993)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
US 6000610 A	December 14, 1999		014	G06K015/00

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
US 6000610A	February 26, 1993	1993US-0023955	

INT-CL (IPC): G06 K 15/00

ABSTRACTED-PUB-NO: US 6000610A
BASIC-ABSTRACT:

NOVELTY - A portable shopping map (10) includes a display surface (11) bearing store specific indicia arranged in a pictorial representation (12) of several aisle locations (14) in store. The portable map is usable as a shopping list for selecting discrete articles for purchase from store and as an in-store map for locating selected discrete articles in the shop.

DETAILED DESCRIPTION - The store specific indicia comprises written identifications (16) with detailed descriptions of discrete articles. An INDEPENDENT CLAIM is also included for shoppers aiding method.

USE - For aiding shoppers in selection and location of articles displayed for sale at various aisle location in stores such as large sale one-stop shopping stores.

ADVANTAGE - Enables shopper to organize and plan for a shopping trip, away from store such as at home to minimize time spent in the stores, by providing portable map.

DESCRIPTION OF DRAWING(S) - The figure shows the illustration of shopping map.

Portable shopping map 10

Display surface 11

Pictorial representation 12

Aisle locations 14

Identifications 16

ABSTRACTED-PUB-NO: US 6000610A
EQUIVALENT-ABSTRACTS:

CHOSEN-DRAWING: Dwg.1/8

DERWENT-CLASS: T01
EPI-CODES: T01-J05A1;

Previous Doc Next Doc Go to Doc#

L43: Entry 2 of 3 File: TDBD Dec 1, 1999

TDB-ACC-NO: NNRD428118

DISCLOSURE TITLE: Customer Premises Equipment Providing Wireless Clients Access to Consolidated Broadband Services

PUBLICATION-DATA:
IBM technical Disclosure Bulletin, December 1999, UK

ISSUE NUMBER: 428
PAGE NUMBER: 1682

PUBLICATION-DATE: December 1, 1999 (19991201)

CROSS REFERENCE: 0374-4353-0-428-1682

DISCLOSURE TEXT:

Disclosed is equipment that connects wireless devices on the customer premises to a broadband network using standard wireless protocols. A preferred embodiment uses the wireless protocols defined by the Bluetooth (TM) Special Interest Group; see www.bluetooth.com for details. The term "broadband network" includes, but is not limited to, the cable television cable plant, asymmetrical digital subscriber line (ADSL) connected to a telephone carrier's local loop, digital satellite television transmissions, and wireless bypass to a local carrier's point of presence using a broadband wireless technology such as LMDS.

The equipment, including hardware and software, is a set-top box or customer-premises equipment that provides the consumer with a single access point for telephone, Internet, cable TV, video-on-demand, music-on-demand, radio programming, and other new telecommunication and network services. This invention is also a key integration platform to integrate these services and provide "one-stop shopping" to the telecommunications consumer.

Client devices that may wirelessly access broadband services using this invention include but are not limited to telephone base stations, telephone handsets, and audio headsets; audiovisual equipment including televisions, video cassette recorders, digital cameras, video cameras, stereo receivers, and remote controls for all of the same; input devices such as a keyboard, keypad, mouse, touch-screen, or other pointing device; and computers of all kinds, including personal, notebook, subnotebook, palmtop, and personal digital assistant; home security systems, video monitors, motion sensors, switches, lights; and so forth. Telecommunications industry analysts used to talk about "the last mile" and speculate about when fiber deployment to the home would become a reality. The battleground has shifted from the "last mile" to the radio frequency spectrum inside the home or office, and the access point where the local piconet connects to the broadband network. Carriers are jockeying for position to offer single-stop shopping to the consumer. The chairman of one telecommunications giant said that his company wants to offer wireline telephone, internet, wireless cellular, and cable TV services for a single price. That company's recent acquisitions of cellular properties and entry back into local phone service makes that clear. It is also evident that the largest software vendors are focusing on the low-end single-set-top-box market in

underdeveloped countries, as well as taking equity positions in telecommunications companies. One large internet service provider was recently disappointed by its failure to win an acquisition bid for a CATV giant, and is now seeking an equity position in a digital television broadcasting system that could deliver downstream content over 9 million subscribers' digital satellite TV dishes and upstream data over land-lines.

The Bluetooth (TM) standard, operating worldwide in the unlicensed 2.4 GHz band (or a similar short-range low-power standard digital wireless technology that can tolerate moderate interference) is the key technology that will make such single-access-point carrier services possible. Bluetooth Version 1 supports asynchronous data rates of 762 kbps per picocell, over a 10-meter range with a 0 dBm radio transmitter, or over a 100-meter range with a 20 dBm radio transmitter. Up to 10 picocells can coexist within radio proximity, due to the use of a frequency-hopping spread-spectrum baseband technolog characterized by graceful degradation as additional contending transmitters are added. Alternatively it can support up to 3 isochronous 64 kbps connections per picocell.

Some of the devices that can be wirelessly attached to the broadband network using Bluetooth standards are discussed below: Telephone handsets. Consumers will be reluctant to rewire their homes to give their telephones access to the broadband network; but it won't be necessary. If the CPE is a "set-top box" near the TV (as it must be today, so the consumer can control the TV with an infrared remote control), then consumers will buy wireless telephone handsets (rather than run new wiring from the CPE to the locations of telephones within the home). The CPE will include the functions of a cordless telephone base station. Cordless handsets -- using proprietary radio technology operating in the 900 MHz band or other unlicensed RF spectrum -- are already commonly available. The Bluetooth standard defines several telephony functions supporting multiple 64kbps voice channels between a handset and a base station, between two compatible handsets (termed 3-in-1 phones), or between a wireless headset and a telephone handset. The standard als supports "modem emulation" so that a computer can access a cordless telephone wirelessly. Television remote control or entry-level network input device.

Implementing the remote control for the CPE and other audiovisual equipment using an RF standard (such as Bluetooth) removes the constrain that the CPE be physically adjacent to the customer's equipment, TV, computer, or telephone base station. Instead, the CPE can be situated where the broadband service enters the home, i.e. on the outside of the building (the same place where an ADSL transceiver, telephone patch-panel, or CATV splitter, would be deployed). Such outside deployment facilitates service installation and maintenance. This type of CPE must be powered. Power could be supplied by a connection to the A/C service; a low DC voltage provided by the current public switched telephone network; or an inexpensive rechargeable battery such as a lithium-ion or similar battery intended for use in mobile computers and cellular telephone handsets, and recharged by trickle-current from a small integrated photovoltaic cell. The use of various wireless transmission between CPE and a keyboard, touch screen, or computer is already known. For example, WebTV uses infrared transmission between a cordless keyboard and a set-top box. An application is available to control a television from a palm-top computer equipped with an infrared port. An RF-based remote control that operates in the ultra-high frequency (UHF) band is available to control certain K- and S-band satellite TV receivers, enabling the consumer to change channels and steer the satellite dish from anywhere in range of the remote. RF overcomes the line-of-sight limitation of infrared technology. This invention improves remote control technology by wirelessly transmitting program listings, movie reviews, and the like from the CPE to a hand-held mobile-computer remote-control so the consumer can select specific programs by category or content, rather than selecting channels by number as is done today. The consumer could also interact with the Internet using such a wireless device. Computer. Computers can connect to the CPE via wiring suitable for Ethernet (standard on many new homes) using standard Ethernet or 802.3

protocols. Ethernet is the standard way to access either asymmetric digital subscriber line (ADSL) or cable modem. Alternatively, computers can access the CPE over a wireless connection such as by using the Bluetooth "LAN Access using PPP" standard. Migration to this new scheme will not happen quickly. Some migration will not occur until higher wireless speeds of 4-20 megabits per second are available. And mass migration from existing telephones and handsets will take 10+ years. But high-end consumers will buy standards-based wireless phones right away, and many already have Ethernet-ready PCs. The 3-in-1 phone will be popular with many consumers and, in fact, will incent many to buy a compatible phone base station (attached to the existing public switched telephone network, or to the broadband network). All client devices will access the broadband network using the same, standard, wireless technology. This means each of these components will be standard and interoperable. This fact has several consequences that increase the value of this invention: The consumer can migrate one piece at a time (lowering the barrier to entry) Sharp competition will keep prices low, benefitting the consumer Manufacturing volume for common price-sensitive components such as radio modules, antennae, and radio chips, will increase, driving prices lower.

A carrier, access provider, or service provider will gain economies of scale by consolidating telephony services, improving the efficiency and cost-effectiveness of the broadband network through higher utilization, as well as providing the ability to purchase, deploy, and manage a smaller number of higher-capacity network components such as switches, repeaters, fiber-optic cables, and multiplexers. This will also improve their ability to offer the consumer "one-stop shopping" for all their telecommunications needs, rather than the consumer getting separate bills for land-line telephone, cellular telephone, cable TV service, satellite TV programming, long-distance telephone, internet access, etc, as is the case today. This in turn will allow the largest providers to offer volume discounts to the best consumers, further increasing the utilization of such services. Information providers will be able to offer value-added combined and integrated services, such as TV program listings displayed on the computer or remote control, video telephone services, voice over IP (where price and quality warrants), automatic program recording and playback, integrated information services such as telephone number lookup over one device followed by automatic dialing of the number by the CPE device, etc.

Previous Doc Next Doc Go to Doc#

L40: Entry 3 of 3 File: USPT Feb 5, 2002

US-PAT-NO: 6345239
DOCUMENT-IDENTIFIER: US 6345239 B1

TITLE: Remote demonstration of business capabilities in an e-commerce environment

DATE-ISSUED: February 5, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Bowman-Amuah; Michel K.	Colorado Springs	CO		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Accenture LLP	Palo Alto	CA			02

APPL-NO: 09/ 388026 [PALM]
DATE FILED: August 31, 1999

INT-CL: [07] G06 G 7/48

US-CL-ISSUED: 703/6; 705/26, 705/39
US-CL-CURRENT: 703/6; 705/26, 705/39

FIELD-OF-SEARCH: 703/1, 703/2, 703/6, 703/13, 703/23, 705/26, 705/27, 705/39

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5295244	March 1994	Dev et al.	395/161
☐	5461611	October 1995	Drake, Jr. et al.	370/54
☐	5652787	July 1997	O'Kelly	379/112
☐	5694548	December 1997	Baugher et al.	395/200
☐	5864823	January 1999	Levitan	105/14
☐	5944795	August 1999	Civanlar	709/227
☐	6026376	February 2000	Kenney	705/27
☐	6052670	April 2000	Johnson	705/27

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0941010	September 1999	EP	
0944209	September 1999	EP	
WO 98/18237	April 1998	WO	
WO 99/34587	July 1999	WO	

OTHER PUBLICATIONS

Parker et al, "An Internet-Mediated Business Simulation: Developing and Using TRECS", Simulation & Gaming, vol. 30 No. 1, pp. 51-69, Mar. 1999.*
Zack, "An MIS Course Integrating Information Technology and Organizational Issues", Database for Advances in Information Systems, pp. 73-87 (Spring 1998).*
Paul et al, "Simulation of Business Processes", American Behavioral Scientist, pp. 1551-1576, Aug. 1999.*
Maren S. Leizaola, Tuning IP Performance: The Right Tools for the Task, May 1998 URL: http://data.com/tutorials/tuning.html, Viewed Oct. 15,1999.
Mick Seaman et al., Going the Distance with QOS, Feb. 1999, URL, http://data.com/issue/990207/distance.html, Viewed Oct. 15, 1999.
Stephen Saunders, The Policy Makers, May 1999, URL,http://data.com/issue/990507/policy.html, Viewed Oct. 15, 1999.

ART-UNIT: 2123

PRIMARY-EXAMINER: Teska; Kevin J.

ASSISTANT-EXAMINER: Broda; Samuel

ATTY-AGENT-FIRM: Burton; Daphne Oppenheimer Wolff & Donnelly LLP

ABSTRACT:

A system, method and article of manufacture are provided for demonstrating business capabilities in an e-commerce environment. Data connectivity is first provided between a plurality of sites on a network, which are located in distinct geographic locations. Demonstration data, which illustrates business capabilities of one of the sites, is then received from one of the sites. Thereafter, the demonstration data is organized in a demonstration format and transmitted over the network in the demonstration format to another of the sites.

18 Claims, 110 Drawing figures

Previous Doc Next Doc Go to Doc#

L40: Entry 1 of 3 File: USPT Aug 12, 2003

US-PAT-NO: 6606744
DOCUMENT-IDENTIFIER: US 6606744 B1
**** See image for Certificate of Correction ****

TITLE: Providing collaborative installation management in a network-based supply chain environment

DATE-ISSUED: August 12, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Mikurak; Michael G.	Hamilton	NJ		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Accenture, LLP	Palo Alto	CA			02

APPL-NO: 09/ 444654 [PALM]
DATE FILED: November 22, 1999

INT-CL: [07] G06 F 9/445

US-CL-ISSUED: 717/174; 717/174, 717/178, 705/26
US-CL-CURRENT: 717/174; 705/26, 717/178

FIELD-OF-SEARCH: 717/168, 717/170, 717/171, 717/174, 717/177, 717/172, 717/102, 717/176, 717/178, 705/1, 705/21, 705/26, 705/28, 709/201, 709/217, 709/227

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4491947	January 1985	Frank	
☐	4972453	November 1990	Daniel et al.	
☐	5109337	April 1992	Ferriter et al.	
☐	5159685	October 1992	Kung	
☐	5297031	March 1994	Gutterman et al.	
☐	5483637	January 1996	Winokur et al.	
☐	5495610	February 1996	Shing et al.	709/221

☐	5513343	April 1996	Sakano et al.	
☐	5539877	July 1996	Winokur et al.	
☐	5611048	March 1997	Jacobs et al.	713/202
☐	5621663	April 1997	Skagerling	
☐	5646864	July 1997	Whitney	
☐	5655068	August 1997	Opoczynksi	
☐	5694546	December 1997	Reisman	
☐	5696975	December 1997	Moore et al.	717/168
☐	5729735	March 1998	Meyering	
☐	5761502	June 1998	Jacobs	
☐	5764543	June 1998	Kennedy	
☐	5768501	June 1998	Lewis	
☐	5819028	October 1998	Manghirmalani et al.	
☐	5832196	November 1998	Croslin et al.	
☐	5864483	January 1999	Brichta	
☐	5864662	January 1999	Brownmiller et al.	
☐	5883955	March 1999	Ronning	
☐	5890175	March 1999	Wong et al.	
☐	5893905	April 1999	Main et al.	
☐	5895454	April 1999	Harrington	
☐	5907490	May 1999	Oliver	
☐	5953707	September 1999	Huang et al.	
☐	5974391	October 1999	Hongawa	
☐	5974395	October 1999	Bellini et al.	705/9
☐	5974403	October 1999	Takriti et al.	
☐	5987423	November 1999	Arnold et al.	
☐	5999525	December 1999	Krishnaswamy et al.	
☐	6006016	December 1999	Faigon et al.	
☐	6006196	December 1999	Feigin et al.	
☐	6058426	May 2000	Godwin et al.	
☐	6067525	May 2000	Johnson et al.	
☐	6104868	August 2000	Peters et al.	
☐	6105069	August 2000	Franklin et al.	709/229
☐	6151582	November 2000	Huang et al.	
☐	6157915	December 2000	Bhaskaran et al.	705/7
☐	6167378	December 2000	Weber, Jr.	
☐	6195697	February 2001	Bowman-Amuah	
	6199204	March 2001	Donohue	717/178

☐				
☐	6219700	April 2001	Chang et al.	709/222
☐	6253339	June 2001	Tse et al.	
☐	6256676	July 2001	Taylor et al.	709/246
☐	6289462	September 2001	McNabb et al.	713/201
☐	6314565	November 2001	Kenner et al.	717/171
☐	6347398	February 2002	Parthasarthy et al.	717/178
☐	6349237	February 2002	Koren et al.	
☐	6470496	October 2002	Kato et al.	717/173
☐	6487718	November 2002	Rodriguez et al.	717/177

OTHER PUBLICATIONS

Tan et al, "Applying component technology to improve global supply chain network management", ACM pp. 296-301, 1999.*
Ball et al, "Supply chian infrastructures system integration and information sharing", ACM SIGMOD, vol. 31, No. 1, pp. 61-66, Mar. 2002.*
Fu et al, "Multi agent enabled modeling and simulation towards collaborative inventory management in supply chains", ACM Proc. winter simulation, pp. 1763-1771, 2000.*
Zhao et al, "Data management issues for large scale distributed wokflow system on the internet", The database for Adv. in Inf. Sys. vo. 29, No. 4, pp. 22-32, 1998.*
"Network Trends: Internet Technology Improves Supply Chain Management". Asia computer Trends. Singapore. Dec. 14, 1998.
"Network Two Chooses Netcool to Support Ongoing Expansion and Proactive Management Initiative", Business Wire, Nov. 2, 1998, 2 pages, [Retrieved on Mar. 19, 2002], Retrieved from: Proquest.
"Proactive Networks Offers TelAlert-Pronto Watch 2.5 Integration", business Wire, Nov. 2, 1998, 2 pages, [Retrieved on Mar. 19, 2002], Retrieved from: Proquest.
"User's Guide for Microsoft Project." 1995; Microsoft Corporation. pp. 3,4,14-16, 82-84, 91, 130, 132-134, 175, 209. Document No. Pj62476-0895.

ART-UNIT: 2122

PRIMARY-EXAMINER: Khatri; Anil

ATTY-AGENT-FIRM: Oppenheimer Wolff & Donnelly, LLP Nader; Rambed

ABSTRACT:

A system, method and article of manufacture are provided for collaborative installation management in a network-based supply chain environment. According to an embodiment of the invention, telephone calls, data and other multimedia information are routed through a network system which includes transfer of information across the internet utilizing telephony routing information and internet protocol address information. The system includes integrated Internet Protocol (IP) telephony services allowing a user of a web application to communicate in an audio fashion in-band without having to pick up another telephone. Users can click a button and go to a call center through the network using IP telephony. The system invokes an IP telephony session simultaneously with the data session, and uses an active directory lookup whenever a user uses the system. Users include service providers and manufacturers utilizing the network-based supply chain environment.

L42: Entry 1 of 2 File: USPT Aug 12, 2003

DOCUMENT-IDENTIFIER: US 6606744 B1
** See image for Certificate of Correction **
TITLE: Providing collaborative installation management in a network-based supply chain environment

Drawing Description Text (140):
FIG. 141 is a block diagram of a bill pay system relying on postal mailed payments;

Drawing Description Text (141):
FIG. 142 is a block diagram of a bill pay system wherein consumers pay bills using a bill pay service bureau which has the consumers as customers;

Drawing Description Text (142):
FIG. 143 is a block diagram of a bill pay system where billers initiate automatic debits from consumers' bank accounts.

Detailed Description Text (194):
While there are components in the NGN that ensure interoperability between "NGN" and PSTN, there are alsc a huge new set of new services that are built entirely on the NGN components which is provide feature rich multimedia (voice, video, data) based communication services as well as enabling many E-Commerce services enabled by IP technologies. These components (described later in detail) include directories, policies, user authentication, registration, and encryption. These components enable services like integrated messaging, multimedia conversations, on-demand multi-point conference, enhanced security & authentication, various classes of media transport services, numerous automations in electronic internet commerce activities e.g. banking, shopping, customer care, education, etc. As the NGN matures third party value added service providers will develop IP based services that will combine applications such as electronic commerce (procurement, warehousing, distribution and fulfillment) as well as online banking to present the consumer with an integrated boundless shopping experience.

Detailed Description Text (200):
Given the huge revenues and global nature of PSTN services, as well as their use of SS7 and AIN technologies, components that allow interoperability between "NGN" and PSTN will need to be developed. These will include IP/PSTN Gateways, IP/PSTN address translators, IP/SS7 Gateways, IP enabled SSP's, and IP based Intelligent Peripherals. In addition to IN enablers, new components (as will be describe later) with features like directories, policies, user authentication, registration, session encryption, etc. will also be developed to enhance the IN capabilities. The NGN-IN enablers will provide the next level of intelligence in order to address communication over mixed media types, control of multiple session characteristics, collaborative communications needs, ubiquitous network access, "any to any" communications, and multimedia delivered information services. Note that these "NGN" components will continue to evolve to provide similar and enhanced capabilities in the "New Core".

Detailed Description Text (204):
Example: Assuming a US based NGN service user was roaming in Europe and wanted to

access the network but has the use of specific calling information stored in his profile database in the US, how would such a challenge be overcome without replicating the user's data onto every rules database on the NGN to ensure that the user would not be denied access to features and services which the user typically subscribed. Obviously, storing or replicating this data and then managing synchronicity over a worldwide network would be process intensive, costly and cumbersome. This intelligent network architecture addresses these issues efficiently with mechanisms that make remote data available locally for the duration of a session and then caches the information in short term non-volatile memory not in the foreign rules database server. In other words although a user's profile may be physically stored in a Rules database in the United States, the user may access the network from Europe and be automatically granted access to the specific services and features that normally would be available during his US service experience. The remote session controller in Europe would communicate with the cross network location register and rules database server to identify the subscriber's "home" rules database in order to collect the policies and profile of the subscriber for use in Europe; this is done by using the inter device message sets (command and control) over the control plane sub network. Unlike other mechanisms often employed, this mechanism does not replicate this information onto the local (European) rules database, making long term control data management predictable. The design is CORBA compliant and therefore can be interconnected with other standards based networks.

Detailed Description Text (212):
This process or application is critical since it is the "glue" between the end user application and the communications network. It is responsible for collection and distribution of end-user session preferences, application requirements, access device capability and accounting policy information to the required "IN enabling" components. In summary its main functions are to: Create the AMA/CDR and other usage records Interfaces external 3.sup.rd party Network Gateways. Liase with Clearing Houses and Cross Network Location Registers Feeds the Financial Infrastructure

Detailed Description Text (213):
Cross Network (Roaming) Location Register (Policy Management)

Detailed Description Text (214):
Similar to the Home location register in the wireless/cellular telephony world. This functional component provides the required policies governing users who access third party networks and cross geographical boundaries. It keeps in constant contact with other cross network location registers of the geographically dispersed but inter-connected networks, exchanging accounting, service feature profile and control data for local and roaming subscribers.

Detailed Description Text (262):
FIG. 26 is a flowchart illustrating an Invoice and Collections Process in accordance with a preferred embodiment. First, in step 2600, customer account inquiries and customer payment information is received by the system. Next, in step 2602, billing data, including discounts due to quality of service violations and rebates due to service level agreement violations, is collected and processed. Thereafter, in step 2604, customer account invoices are created for distribution based on the customer payment information and the billing data.

Detailed Description Text (441):
The Internet access software accesses and "handshakes" with an "Internet Entry Server", which verifies the PIN number, provides the access and times the user's access time. The Internet Entry Server is programmed to recognize the PIN number as entitling the user to a limited prepaid or "free" Internet access time for on-line help services. Such a time period could be for a total time period such as 1 hour or more, or access to on-line help services can be unlimited for 90 days, 6 months,

etc., for example, with the access time paid for by the sponsor/vendor. The first time a customer uses the on-line help service, the Internet Entry Server performs a registration process which includes a number of personal questions and custom data gathering in the form of queries provided by the sponsor/vendor for response by the user.

Detailed Description Text (450):
In a lookup step 5108, the telephonic communication over the hybrid network is limited bases on a user profile. Preferably the user profile is included in a rules database. By locating the user profile within the rules database, the rules database can provide seamless cross-location registration without the need for duplicate databases located on different networks. Using a rules database, a user utilizing the Internet in Europe can get the same telephony service as provided in the United States, as described above. Preferably the computer used to interface with the Internet includes multimedia equipment such as speakers and a microphone. Utilizing a multimedia equipped computer allows a user to use telephonic communication with little or no disruption while interfacing with the Internet. Multimedia computer speakers are used to receive the telephony audio from the network and the microphone is used to transmit the telephony data to the network.

Detailed Description Text (509):
WAFF capabilities may be employed, and a WAF agreement may be entered into, by a plurality of parties without the WAFF capabilities being directly associated with the controlling of certain, specific electronic information. For example, certain one or more WAFF capabilities may be present at a WAF installation, and certain WAF agreements may have been entered into during the registration process for a content distribution application, to be used by such installation for securely controlling WAF content usage, auditing, reporting and/or payment. Similarly, a specific WAF participant may enter into a WAF user agreement with a WAF content or electronic appliance provider when the user and/or her appliance register with such provider as a WAF installation and/or user. In such events, WAFF in place control information available to the user WAF installation may require that certain WAFF methods are employed, for example in a certain sequence, in order to be able to use all and/or certain classes, of electronic content and/or WAF applications.

Detailed Description Text (523):
WAF allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. WAF's security and metering secure subsystem core will be present at all physical locations where WAF related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a "virtual black box," a collection of distributed, very secure WAF related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means. WAF further includes highly configurable transaction operating system technology, one or more associated libraries of load modules along with affiliated data, WAF related administration, data preparation, and analysis applications, as well as system software designed to enable WAF integration into host environments and applications. WAF's usage control information, for example, provide for property content and/or appliance related: usage authorization, usage auditing (which may include audit reduction), usage billing, usage payment, privacy filtering, reporting, and security related communication and encryption techniques.

Detailed Description Text (536):
Recently, an online shopping system which allows examination, selection and order of items through a computer has been put into practice. In such an online shopping system, in order to supplement a disadvantage by a gap from ordinary shopping caused by the use of electronic means such as not capable of directly touching the

item and not capable of getting assistance of a real salesman, various devices for a user interface have been made. As one of such devices, a so-called shopping basket function which has some analogy with shopping basket used in a shop such as supermarket is proposed. In this function, items on the online shopping are temporarily added to a purchase list and a process of order and purchase is conducted when all items to be purchased are registered on the list, as items to be purchased in the supermarket are once put into a shopping basket and lastly the account is settled at a counter. In this manner, by preparing the purchase list to order a plurality of items one time, a time required to purchase may be substantially saved. Further, the consumer may prevent the failure of shopping and stop the purchase of unnecessary items by checking the list once before the purchase. Further, because of feel of easiness that the items once added on the purchase list may be finally changed in any way before the purchase, there is a psychological effect that the consumer may proceed shopping readily.

Detailed Description Text (542):
In accordance with the present invention, an interface for providing the shopping basket function is provided as a separate shopping basket window from a catalog window on which online shop item data is displayed. The shopping basket window is displayed on the catalog window and a display position is moved in linkage with the movement of a mouse pointer. The shopping basket includes a list of items to be purchased which is a main body of the shopping basket, a function to add the item data to the list, and a function to change the item data registered in the list. In one embodiment of the present invention, the shopping basket main body is not always displayed. Instead, an interface function to display the shopping basket contents on the screen is provided on the shopping basket window.

Detailed Description Text (565):
Home Banking bill payment services are examples of an EFT system used by individuals to make payments from a home computer. Currently, home banking initiatives have found few customers. Of the banks that have offered services for payments, account transfers and information over the telephone lines using personal computers, less than one percent of the bank's customers are using the service. One reason that Home Banking has not been a successful product is because the customer cannot deposit and withdraw money as needed in this type of system.

Detailed Description Text (679):
The second aspect of the invention is the governing logic for controlling system dynamics. This logic is stored in system memory and provides the sequence of protocols and rules that allocate trading priority, and the system responses to operative commands entered by the brokers at the workstations. The system logic is critical on two levels. First, it is important as the guiding principles underlying the system and thus performance is tied directly thereto. On a second level, system logic must be known to all customers and traders as the rules dictating market access and response--to eliminate any confusion and to place participants on as close to an equal footing as possible. It is a fundamental precept of the present system to provide fair and complete access to the trading process to all registered participants.

Detailed Description Text (715):
LEGAL SERVICES Lists legal policies and notifications (privacy policy) Accepts notification of legal questions or issues Provides media kits Allows users to register for branding usage

Detailed Description Text (716):
Legal notices and policies are displayed by the content channels component of the present invention. Legal questions and issues are accepted and stored for later reply. A user is also allowed to register for branding usage. Media kits may be provided.

Detailed Description Text (718):
As shown in component 5306 of FIG. 53, one embodiment of the present invention is provided for affording a combination of web application services to manage customer relationships. FIG. 67 illustrates component 5306 in more detail. As shown in FIG. 67, profile data of a plurality of users is managed and organized in operation 6700. Static and dynamic information of interest is provided to each user based on profile data of that user in operation 6704. Further, static and dynamic information of interest is provided to a plurality of users having similar profile data in operation 6704. Information is also located on a network of databases, i.e. the Internet, as a function of the profile data. Feedback is also collected from the users by way of electronic forms and surveys Note operation 6706. Various event, calendaring and registration services are further provided. For example, operation 6708 reminds the users of upcoming events, a calendar of events is maintained, and the users are permitted to register for the events.

Detailed Description Text (728):
EVENTS, CALENDARING, AND REGISTRATION Offers user the ability to view upcoming events and register for them online Checks identity of user to authorize registration Checks for relevant events based on user profiles and notifies users Sends out notices to remind users of upcoming events for which user has registered Maintains calendar of events and administration of calendar Integrates with commerce functions to provide fee-based registration capabilities (e.g. online registration via credit card)

Detailed Description Text (729):
Referring to operations 6708, 6800, and 6802 of FIGS. 67 and 68, the customer relationship management component of the present invention includes a calendar of events, a notification service, and a way to register for upcoming events. Relevant events are selected based on the profile of a user and the user is notified of the time and place of the event. Once the identity of a user has been verified, the registration of the user is accepted. A notice is sent to a user to remind the user of the event for which he or she has registered. The registration function is integrated with commerce functions to permit fee-based registration capabilities, such as permitting online registration via credit card.

Detailed Description Text (778):
One embodiment of the present invention is provided for affording a combination of education-related web application services, illustrated as component 5310 of FIG. 53. FIG. 71 provides more detail. In operations 7100 and 7102 respectively, a curriculum of course offerings is generated from which users are permitted to select, i.e. order, register, etc. Education such as training or the like is carried out over a network such as the Internet in operation 7104. At any given time, a status of the education may be provided, including such things as a listing of the courses completed, scores for the courses completed, a listing of courses for which currently enrolled and the current scores in those courses, a listing of courses required to matriculate, etc. Note operation 7106.

Detailed Description Text (953):
REGISTER FOR TRAINING AND ORDER TRAINING Provides an interactive interface to register for all offerings Integrates with commerce functions to provide order placement and transaction processing (e.g. Takes orders online by credit card) Allows users to register for third party training Allows users to register for online training Supports multiple payment options Integrates with third party systems

Detailed Description Text (954):
Users may order and register for any educational offering on an interactive interface through operation 7102 of FIG. 71. Examples of offerings may include third party training and online training. The interactive interface may be integrated with the commerce component to permit transactional processing when

placing an order. For example, a user may sign up for an offered course and pay the tuition by credit card. Alternatively, the commerce component could create a payment schedule which requires that payments be made periodically. Optionally, the registration and ordering components are able to integrate with third party service providers' systems.

Detailed Description Text (960):
Referring to component 5312 of FIG. 53, one embodiment of the present invention is provided for affording a combination of customer-related web application services to support a product. More detail is provided in FIG. 74. In operation 7400, a user is allowed to register the product. Further, on-line support information is provided about the product. Such support information is provided based on queries. Note operation 7402. As an option, this information may also be afforded by way of a specially managed call center. In addition, in operation 7404, claims may be handled relating to the product. During operation 7406, the users are automatically notified of upgrades and/or problems relating to the product. Consulting services may also be made available.

Detailed Description Text (961):
PRODUCT REGISTRATION Allows customers to register products online Automatically sends users confirmation of registration Notifies users of upgrades or other product-related information Maintains database on user's purchases to create profiles

Detailed Description Text (962):
Operation 7400 of the web customer service component of the present invention allows the registration of a product, preferably online. Upon registration of a product, confirmation that the registration has been received is automatically sent to the user, such as by email. Notices of upgrades, promotions, and other product-related information is sent to registered users. A database stores the purchases of each user to create profiles, which may be used statistically for marketing purposes.

Detailed Description Text (986):
RETURNS AND WARRANTY CLAIMS Lists warranties Automatically checks user identity to validate user is registered Checks claim to see if it matches warranty criteria Request automatically routed to appropriate agent

Detailed Description Text (987):
The web customer service component of the present invention lists warranties for view by a user in operation 7404 of FIG. 74. When a user has a product that requires service or return under the warranty, the identity of the user is checked to ensure that the user has registered. The claim made by the user is then checked and compared to the warranty to ensure that the claim meet warranty criteria for the requested service or replacement. Once validated, the claim is routed to the appropriate agent.

Detailed Description Text (991):
PROACTIVE SERVICE NOTIFICATION Automatically notifies registered customers about needed and optional upgrades Automatically notifies registered customers about possible bugs or problems and suggested solutions

Detailed Description Text (992):
One embodiment of the present invention is provided for affording proactive customer support. Registered users are automatically notified about necessary and optional upgrades. See operation 7406 of FIG. 74. Optionally, a description of the upgrade may be included with the notification, along with recommendations about whether or not to install the upgrade. Further, registered users are automatically notified of possible problems or bugs and solutions are suggested, such as configuration changes or downloads.

Detailed Description Text (994):
In use, a user enters the system by purchasing products and/or services through a website. As part of the purchase transaction or product registration, the user defines the products and services which the user currently possesses or purchases by completing a user profile (user indicia). Incentives and disincentives may be used to influence the user indicia that is entered. Then, the user defines his specific desires for support including: levels of support, support channel, methods of use of the products and services and future purchasing plans (additional user indicia), which are received in operation 7503. The products and services which the user identified and/or purchased are monitored through the internet and other means in operation 7504. For example, search engines may scan provider websites for updates and patches, reduced price offerings, etc. Further, a dedicated email address corresponding to the user may be used when registering the product with the manufacturer, thereby providing a central location to receive notices and promotional material. If an issue with a product is found in operation 7505 such as a software bug, a factory recall or a reduced price offering, then the user is notified utilizing his defined channel such as mail, email, fax, telephone in operation 7506. If the user encounters an issue and requests support, the support will be provided utilizing the user's preferred channel and at the support level purchased by the user.

Detailed Description Text (1024):
WAF, for example, can employ: (1) Secure metering means for budgeting and/or auditing electronic content and/or appliance usage; (2) Secure flexible means for enabling compensation and/or billing rates for content and/or appliance usage, including electronic credit and/or currency mechanisms for payment means; (3) Secure distributed database means for storing control and usage related information (and employing validated compartmentalization and tagging schemes); (4) Secure electronic appliance control means; (5) A distributed, secure, "virtual black box" comprised of nodes located at every user (including WAF content container creators, other content providers, client users, and recipients of secure WAF content usage information) site. The nodes of said virtual black box normally include a secure subsystem having at least one secure hardware element (a semiconductor element or other hardware module for securely executing WAF control processes), said secure subsystems being distributed at nodes along a pathway of information storage, distribution, payment, usage, and/or auditing. In some embodiments, the functions of said hardware element, for certain or all nodes, may be performed by software, for example, in host processing environments of electronic appliances; (6) Encryption and decryption means; (7) Secure communications means employing authentication, digital signaturing, and encrypted transmissions. The secure subsystems at said user nodes utilize a protocol that establishes and authenticates each node's and/or participant's identity, and establishes one or more secure host-to-host encryption keys for communications between the secure subsystems; and (8) Secure control means that can allow each WAF installation to perform WAF content authoring (placing content into WAF containers with associated control information), content distribution, and content usage; as well as clearinghouse and other administrative and analysis activities employing content usage information.

Detailed Description Text (1030):
The security component of the present invention verifies user identity using built-in browser functionality, allowing for immediate access to a user without requiring installation of additional software. Authentication information may be maintained throughout selected or all sessions to prevent unauthorized users from accessing resources through a registered user's connection.

Detailed Description Text (1169):
Use of bitmap meters (including "regular" and "wide" bitmap meters) to record usage and/or purchase of information, in conjunction with other elements of the preferred embodiment of the present invention, uniquely supports efficient maintenance of

usage history for: (a) rental, (b) flat fee licensing or purchase, (c) licensing or purchase discounts based upon historical usage variables, and (d) reporting to users in a manner enabling users to determine whether a certain item was acquired, or acquired within a certain time period (without requiring the use of conventional database mechanisms, which are highly inefficient for these applications). Bitmap meter methods record activities associated with electronic appliances, properties, objects, or portions thereof, and/or administrative activities that are independent of specific properties, objects, etc., performed by a user and/or electronic appliance such that a content and/or appliance provider and/or controller of an administrative activity can determine whether a certain activity has occurred at some point, or during a certain period, in the past (for example, certain use of a commercial electronic content product and/or appliance). Such determinations can then be used as part of pricing and/or control strategies of a content and/or appliance provider, and/or controller of an administrative activity. For example, the content provider may choose to charge only once for access to a portion of a property, regardless of the number of times that portion of the property is accessed by a user. support "launchable" content, that is content that can be provided by a content provider to an end-user, who can then copy or pass along the content to other end-user parties without requiring the direct participation of a content provider to register and/or otherwise initialize the content for use. This content goes "out of (the traditional distribution) channel" in the form of a "traveling object." Traveling objects are containers that securely carry at least some permissions information and/or methods that are required for their use (such methods need not be carried by traveling objects if the required methods will be available at, or directly available to a destination WAF installation). Certain travelling objects may be used at some or all WAF installations of a given WAF arrangement since they can make available the content control information necessary for content use without requiring the involvement of a commercial WAF value chain participant or data security administrator (e.g. a control officer or network administrator). As long as traveling object control information requirements are available at the user WAF installation secure subsystem (such as the presence of a sufficient quantity of financial credit from an authorized credit provider), at least some travelling object content may be used by a receiving party without the need to establish a connection with a remote WAF authority (until, for example, budgets are exhausted or a time content usage reporting interval has occurred). Traveling objects can travel "out-of-channel," allowing, for example, a user to give a copy of a traveling object whose content is a software program, a movie or a game, to a neighbor, the neighbor being able to use the traveling object if appropriate credit (e.g. an electronic clearinghouse account from a clearinghouse such as VISA or AT&T) is available. Similarly, electronic information that is generally available on an Internet, or a similar network, repository might be provided in the form of a traveling object that can be downloaded and subsequently copied by the initial downloader and then passed along to other parties who may pass the object on to additional parties. provide very flexible and extensible user identification according to individuals, installations, by groups such as classes, and by function and hierarchical identification employing a hierarchy of levels of client identification (for example, client organization ID, client department ID, client network ID, client project ID, and client employee ID, or any appropriate subset of the above). provide a general purpose, secure, component based content control and distribution system that functions as a foundation transaction operating system environment that employs executable code pieces crafted for transaction control and auditing. These code pieces can be reused to optimize efficiency in creation and operation of trusted, distributed transaction management arrangements. WAF supports providing such executable code in the form of "atomic" load modules and associated data. Many such load modules are inherently configurable, aggregatable, portable, and extensible and singularly, or in combination (along with associated data), run as control methods under the WAF transaction operating environment. WAF can satisfy the requirements of widely differing electronic commerce and data security applications by, in part, employing this general purpose transaction management foundation to securely process WAF

transaction related control methods. Control methods are created primarily through the use of one or more of said executable, reusable load module code pieces (normally in the form of executable object components) and associated data. The component nature of control methods allows the present invention to efficiently operate as a highly configurable content control system. Under the present invention, content control models can be iteratively and asynchronously shaped, and otherwise updated to accommodate the needs of WAF participants to the extent that such shaping and otherwise updating conforms to constraints applied by a WAF application, if any (e.g., whether new component assemblies are accepted and, if so, what certification requirements exist for such component assemblies or whether any or certain participants may shape any or certain control information by selection amongst optional control information (permissions record) control methods. This iterative (or concurrent) multiple participant process occurs as a result of the submission and use of secure, control information components (executable code such as load modules and/or methods, and/or associated data). These components may be contributed independently by secure communication between each control information influencing WAF participant's WAF installation and may require certification for use with a given application, where such certification was provided by a certification service manager for the WAF arrangement who ensures secure interoperability and/or reliability (e.g., bug control resulting from interaction) between appliances and submitted control methods. The transaction management control functions of a WAF electronic appliance transaction operating environment interact with non-secure transaction management operating system functions to properly direct transaction processes and data related to electronic information security, usage control, auditing, and usage reporting. WAF provides the capability to manages resources related to secure WAF content and/or appliance control information execution and data storage. facilitate creation of application and/or system functionality under WAF and to facilitate integration into electronic appliance environments of load modules and methods created under the present invention. To achieve this, WAF employs an Application Programmer's Interface (API) and/or a transaction operating system (such as a ROS) programming language with incorporated functions, both of which support the use of capabilities and can be used to efficiently and tightly integrate WAF functionality into commercial and user applications. support user interaction through: (a) "Pop-Up" applications which, for example, provide messages to users and enable users to take specific actions such as approving a transaction, (b) stand-alone WAF applications that provide administrative environments for user activities such as: end-user preference specifications for limiting the price per transaction, unit of time, and/or session, for accessing history information concerning previous transactions, for reviewing financial information such as budgets, expenditures (e.g. detailed and/or summary) and usage analysis information, and (c) WAF aware applications which, as a result of the use of a WAF API and/or a transaction management (for example, ROS based) programming language embeds WAF "awareness" into commercial or internal software (application programs, games, etc.) so that WAF user control information and services are seamlessly integrated into such software and can be directly accessed by a user since the underlying functionality has been integrated into the commercial software's native design. For example, in a WAF aware word processor application, a user may be able to "print" a document into a WAF content container object, applying specific control information by selecting from amongst a series of different menu templates for different purposes (for example, a confidential memo template for internal organization purposes may restrict the ability to "keep," that is to make an electronic copy of the memo). employ "templates" to ease the process of configuring capabilities of the present invention as they relate to specific industries or businesses. Templates are applications or application add-ons under the present invention. Templates support the efficient specification and/or manipulation of criteria related to specific content types, distribution approaches, pricing mechanisms, user interactions with content and/or administrative activities, and/or the like. Given the very large range of capabilities and configurations supported by the present invention, reducing the range of configuration opportunities to a manageable subset

particularly appropriate for a given business model allows the full configurable power of the present invention to be easily employed by "typical" users who would be otherwise burdened with complex programming and/or configuration design responsibilities template applications can also help ensure that WAF related processes are secure and optimally bug free by reducing the risks associated with the contribution of independently developed load modules, including unpredictable aspects of code interaction between independent modules and applications, as well as security risks associated with possible presence of viruses in such modules. WAF, through the use of templates, reduces typical user configuration responsibilities to an appropriately focused set of activities including selection of method types (e.g. functionality) through menu choices such as multiple choice, icon selection, and/or prompting for method parameter data (such as identification information, prices, budget limits, dates, periods of time, access rights to specific content, etc.) that supply appropriate and/or necessary data for control information purposes. By limiting the typical (non-programming) user to a limited subset of configuration activities whose general configuration environment (template) has been preset to reflect general requirements corresponding to that user, or a content or other business model can very substantially limit difficulties associated with content containerization (including placing initial control information on content), distribution, client administration, electronic agreement implementation, end-user interaction, and clearinghouse activities, including associated interoperability problems (such as conflicts resulting from security, operating system, and/or certification incompatibilities). Use of appropriate WAF templates can assure users that their activities related to content WAF containerization, contribution of other control information, communications, encryption techniques and/or keys, etc. will be in compliance with specifications for their distributed WAF arrangement. WAF templates constitute preset configurations that can normally be reconfigurable to allow for new and/or modified templates that reflect adaptation into new industries as they evolve or to reflect the evolution or other change of an existing industry. For example, the template concept may be used to provide individual, overall frameworks for organizations and individuals that create, modify, market, distribute, consume, and/or otherwise use movies, audio recordings and live performances, magazines, telephony based retail sales, catalogs, computer software, information data bases, multimedia, commercial communications, advertisements, market surveys, infomercials, games, CAD/CAM services for numerically controlled machines, and the like. As the context surrounding these templates changes or evolves, template applications provided under the present invention may be modified to meet these changes for broad use, or for more focused activities. A given WAF participant may have a plurality of templates available for different tasks. A party that places content in its initial WAF container may have a variety of different, configurable templates depending on the type of content and/or business model related to the content. An end-user may have different configurable templates that can be applied to different document types (e-mail, secure internal documents, database records, etc.) and/or subsets of users (applying differing general sets of control information to different bodies of users, for example, selecting a list of users who may, under certain preset criteria, use a certain document). Of course, templates may, under certain circumstances have fixed control information and not provide for user selections or parameter data entry. support plural, different control models regulating the use and/or auditing of either the same specific copy of electronic information content and/or differently regulating different copies (occurrences) of the same electronic information content. Differing models for billing, auditing, and security can be applied to the same piece of electronic information content and such differing sets of control information may employ, for control purposes, the same, or differing, granularities of electronic information control increments. This includes supporting variable control information for budgeting and auditing usage as applied to a variety of predefined increments of electronic information, including employing a variety of different budgets and/or metering increments for a given electronic information deliverable for: billing units of measure, credit limit, security budget limit and security content metering increments, and/or market

surveying and customer profiling content metering increments. For example, a CD-ROM disk with a database of scientific articles might be in part billed according to a formula based on the number of bytes decrypted, number of articles containing said bytes decrypted, while a security budget might limit the use of said database to no more than 5% of the database per month for users on the wide area network it is installed on. provide mechanisms to persistently maintain trusted content usage and reporting control information through both a sufficiently secure chain of handling of content and content control information and through various forms of usage of such content wherein said persistence of control may survive such use. Persistence of control includes the ability to extract information from a WAF container object by creating a new container whose contents are at least in part secured and that contains both the extracted content and at least a portion of the control information which control information of the original container and/or are at least in part produced by control information of the original container for this purpose and/or WAF installation control information stipulates should persist and/or control usage of content in the newly formed container. Such control information can continue to manage usage of container content if the container is "embedded" into another WAF managed object, such as an object which contains plural embedded WAF containers, each of which contains content derived (extracted) from a different source. enables users, other value chain participants (such as clearinghouses and government agencies), and/or user organizations, to specify preferences or requirements related to their use of electronic content and/or appliances. Content users, such as end-user customers using commercially distributed content (games, information resources, software programs, etc.), can define, if allowed by senior control information, budgets, and/or other control information, to manage their own internal use of content. Uses include, for example, a user setting a limit on the price for electronic documents that the user is willing to pay without prior express user authorization, and the user establishing the character of metering information he or she is willing to allow to be collected (privacy protection). This includes providing the means for content users to protect the privacy of information derived from their use of a WAF installation and content and/or appliance usage auditing. In particular, WAF can prevent information related to a participant's usage of electronic content from being provided to other parties without the participant's tacit or explicit agreement. provide mechanisms that allow control information to "evolve" and be modified according, at least in part, to independently, securely delivered further control information. Said control information may include

Detailed Description Text (1172):
Such aggregation, in the preferred embodiment of the present invention, may involve preserving at least a portion of the control information (e.g., executable code such as load modules) for each of various of said portions by, for example, embedding some or all of such portions individually as WAF content container objects within an overall WAF content container and/or embedding some or all of such portions directly into a WAF content container. In the latter case, content control information of said content container may apply differing control information sets to various of such portions based upon said portions original control information requirements before aggregation. Each of such embedded WAF content containers may have its own control information in the form of one or more permissions records. Alternatively, a negotiation between control information associated with various aggregated portions of electronic content, may produce a control information set that would govern some or all of the aggregated content portions. The WAF content control information produced by the negotiation may be uniform (such as having the same load modules and/or component assemblies, and/or it may apply differing such content control information to two or more portions that constitute an aggregation of WAF controlled content such as differing metering, budgeting, billing and/or payment models. For example, content usage payment may be automatically made, either through a clearinghouse, or directly, to different content providers for different potions. enable flexible metering of, or other collection of information related to, use of electronic content and/or

electronic appliances. A feature of the present invention enables such flexibility of metering control mechanisms to accommodate a simultaneous, broad array of: (a) different parameters related to electronic information content use; (b) different increment units (bytes, documents, properties, paragraphs, images, etc.) and/or other organizations of such electronic content; and/or (c) different categories of user and/or WAF installation types, such as client organizations, departments, projects, networks, and/or individual users, etc. This feature of the present invention can be employed for content security, usage analysis (for example, market surveying), and/or compensation based upon the use and/or exposure to WAF managed content. Such metering is a flexible basis for ensuring payment for content royalties, licensing, purchasing, and/or advertising. A feature of the present invention provides for payment means supporting flexible electronic currency and credit mechanisms, including the ability to securely maintain audit trails reflecting information related to use of such currency or credit. WAF supports multiple differing hierarchies of client organization control information wherein an organization client administrator distributes control information specifying the usage rights of departments, users, and/or projects. Likewise, a department (division) network manager can function as a distributor (budgets, access rights, etc.) for department networks, projects, and/or users, etc. provide scalable, integratable, standardized control means for use on electronic appliances ranging from inexpensive consumer (for example, television set-top appliances) and professional devices (and hand-held PDAS) to servers, mainframes, communication switches, etc. The scalable transaction management/auditing technology of the present invention will result in more efficient and reliable interoperability amongst devices functioning in electronic commerce and/or data security environments. As standardized physical containers have become essential to the shipping of physical goods around the world, allowing these physical containers to universally "fit" unloading equipment, efficiently use truck and train space, and accommodate known arrays of objects (for example, boxes) in an efficient manner, so WAF electronic content containers may, as provided by the present invention, be able to efficiently move electronic information content (such as commercially published properties, electronic currency and credit, and content audit information), and associated content control information, around the world. Interoperability is fundamental to efficient electronic commerce. The design of the WAF foundation, WAF load modules, and WAF containers, are important features that enable the WAF node operating environment to be compatible with a very broad range of electronic appliances. The ability, for example, for control methods based on load modules to execute in very "small" and inexpensive secure sub-system environments, such as environments with very little read/write memory, while also being able to execute in large memory sub-systems that may be used in more expensive electronic appliances, supports consistency across many machines. This consistent WAF operating environment, including its control structures and container architecture, enables the use of standardized WAF content containers cross a broad range of device types and host operating environments. Since WAF capabilities can be seamlessly integrated as extensions, additions, and/or modifications to fundamental capabilities of electronic appliances and host operating systems, WAF containers, content control information, and the WAF foundation will be able to work with many device types and these device types will be able to consistently and efficiently interpret and enforce WAF control information. Through this integration users can also benefit from a transparent interaction with many of the capabilities of WAF. WAF integration with software operating on a host electronic appliance supports a variety of capabilities that would be unavailable or less secure without such integration. Through integration with one or more device applications and/or device operating environments, many capabilities of the present invention can be presented as inherent capabilities of a given electronic appliance, operating system, or appliance application. For example, features of the present invention include: (a) WAF system software to in part extend and/or modify host operating systems such that they possesses WAF capabilities, such as enabling secure transaction processing and electronic information storage; (b) one or more application programs that in part represent

tools associated with WAF operation; and/or (c) code to be integrated into application programs, wherein such code incorporates references into WAF system software to integrate WAF capabilities and makes such applications WAF aware (for example, word processors, database retrieval applications, spreadsheets, multimedia presentation authoring tools, film editing software, music editing software such as MIDI applications and the like, robotics control systems such as those associated with CAD/CAM environments and NCM software and the like, electronic mail systems, teleconferencing software, and other data authoring, creating, handling, and/or usage applications including combinations of the above). These one or more features (which may also be implemented in firmware or hardware) may be employed in conjunction with a WAF node secure hardware processing capability, such as a microcontroller(s), microprocessor(s), other CPU(s) or other digital processing logic. employ audit reconciliation and usage pattern evaluation processes that assess, through certain, normally network based, transaction processing reconciliation and threshold checking activities, whether certain violations of security of a WAF arrangement have occurred. These processes are performed remote to WAF controlled content end-user WAF locations by assessing, for example, purchases, and/or requests, for electronic properties by a given WAF installation. Applications for such reconciliation activities include assessing whether the quantity of remotely delivered WAF controlled content corresponds to the amount of financial credit and/or electronic currency employed for the use of such content. A trusted organization can acquire information from content providers concerning the cost for content provided to a given WAF installation and/or user and compare this cost for content with the credit and/or electronic currency disbursements for that installation and/or user. Inconsistencies in the amount of content delivered versus the amount of disbursement can prove, and/or indicate, depending on the circumstances, whether the local WAF installation has been, at least to some degree, compromised (for example, certain important system security functions, such as breaking encryption for at least some portion of the secure subsystem and/or WAF controlled content by uncovering one or more keys). Determining whether irregular patterns (e.g. unusually high demand) of content usage, or requests for delivery of certain kinds of WAF controlled information during a certain time period by one or more WAF installations and/or users (including, for example, groups of related users whose aggregate pattern of usage is suspicious) may also be useful in determining whether security at such one or more installations, and/or by such one or more users, has been compromised, particularly when used in combination with an assessment of electronic credit and/or currency provided to one or more WAF users and/or installations, by some or all of their credit and/or currency suppliers, compared with the disbursements made by such users and/or installations. support security techniques that materially increase the time required to "break" a system's integrity. This includes using a collection of techniques that minimizes the damage resulting from comprising some aspect of the security features of the present inventions. provide a family of authoring, administrative, reporting, payment, and billing tool user applications that comprise components of the present invention's trusted/secure, universe wide, distributed transaction control and administration system. These components support WAF related: object creation (including placing control information on content), secure object distribution and management (including distribution control information, financial related, and other usage analysis), client internal WAF activities administration and control, security management, user interfaces, payment disbursement, and clearinghouse related functions. These components are designed to support highly secure, uniform, consistent, and standardized: electronic commerce and/or data security pathway(s) of handling, reporting, and/or payment; content control and administration; and human factors (e.g. user interfaces). support the operation of a plurality of clearinghouses, including, for example, both financial and user clearinghouse activities, such as those performed by a client administrator in a large organization to assist in the organization's use of a WAF arrangement, including usage information analysis, and control of WAF activities by individuals and groups of employees such as specifying budgets and the character of usage rights available under WAF for certain groups of and/or individual, client personnel, subject to

control information series to control information submitted by the client administrator. At a clearinghouse, one or more WAF installations may operate together with a trusted distributed database environment (which may include concurrent database processing means). A financial clearinghouse normally receives at its location securely delivered content usage information, and user requests (such as requests for further credit, electronic currency, and/or higher credit limit). Reporting of usage information and user requests can be used for supporting electronic currency, billing, payment and credit related activities, and/or for user profile analysis and/or broader market survey analysis and marketing (consolidated) list generation or other information derived, at least in part, from said usage information. this information can be provided to content providers or other parties, through secure, authenticated encrypted communication to the WAF installation secure subsystems. Clearinghouse processing means would normally be connected to specialized I/O means, which may include high speed telecommunication switching means that may be used for secure communications between a clearinghouse and other WAF pathway participants. securely support electronic currency and credit usage control, storage, and communication at, and between, WAF installations. WAF further supports automated passing of electronic currency and/or credit information, including payment tokens (such as in the form of electronic currency or credit) or other payment information, through a pathway of payment, which said pathway may or may not be the same as a pathway for content usage information reporting. Such payment may be placed into a WAF container created automatically by a WAF installation in response to control information stipulating the "withdrawal" of credit or electronic currency from an electronic credit or currency account based upon an amount owed resulting from usage of WAF controlled electronic content and/or appliances. Payment credit or currency may then be automatically communicated in protected (at least in part encrypted) form through telecommunication of a WAF container to an appropriate party such as a clearinghouse, provider of original property content or appliance, or an agent for such provider (other than a clearinghouse). Payment information may be packaged in said WAF content container with, or without, related content usage information, such as metering information. An aspect of the present invention further enables certain information regarding currency use to be specified as unavailable to certain, some, or all WAF parties ("conditionally" to fully anonymous currency) and/or further can regulate certain content information, such as currency and/or credit use related information (and/or other electronic information usage data) to be available only under certain strict circumstances, such as a court order (which may itself require authorization through the use of a court controlled WAF installation that may be required to securely access "conditionally" anonymous information). Currency and credit information, under the preferred embodiment of the present invention, is treated as administrative content; support fingerprinting (also known as watermarking) for embedding in content such that when content protected under the present invention is released in clear form from a WAF object (displayed, printed, communicated, extracted, and/or saved), information representing the identification of the user and/or WAF installation responsible for transforming the content into clear form is embedded into the released content. Fingerprinting is useful in providing an ability to identify who extracted information in clear form a WAF container, or who made a copy of a WAF object or a portion of its contents. Since the identity of the user and/or other identifying information may be embedded in an obscure or generally concealed manner, in WAF container content and/or control information, potential copyright violators may be deterred from unauthorized extraction or copying. Fingerprinting normally is embedded into unencrypted electronic content or control information, though it can be embedded into encrypted content and later placed in unencrypted content in a secure WAF installation sub-system as the encrypted content carrying the fingerprinting information is decrypted. Electronic information, such as the content of a WAF container, may be fingerprinted as it leaves a network (such as Internet) location bound for a receiving party. Such repository information may be maintained in unencrypted form prior to communication and be encrypted as it leaves the repository. Fingerprinting would preferably take place as the content leaves

the repository, but before the encryption step. Encrypted repository content can be decrypted, for example in a secure WAF sub-system, fingerprint information can be inserted, and then the content can be re-encrypted for transmission. Embedding identification information of the intended recipient user and/or WAF installation into content as it leaves, for example, an Internet repository, would provide important information that would identify or assist in identifying any party that managed to compromise the security of a WAF installation or the delivered content. If a party produces an authorized clear form copy of WAF controlled content, including making unauthorized copies of an authorized clear form copy, fingerprint information would point back to that individual and/or his or her WAF installation. Such hidden information will act as a strong disincentive that should dissuade a substantial portion of potential content "pirates" from stealing other parties electronic information. Fingerprint information identifying a receiving party and/or WAF installation can be embedded into a WAF object before, or during, decryption, replication, or communication of WAF content objects to receivers. Fingerprinting electronic content before it is encrypted for transfer to a customer or other user provides information that can be very useful for identifying who received certain content which may have then been distributed or made available in unencrypted form. This information would be useful in tracking who may have "broken" the security of a WAF installation and was

Detailed Description Text (1173):
illegally making certain electronic content available to others. Fingerprinting may provide additional, available information such as time and/or date of the release (for example extraction) of said content information. Locations for inserting fingerprints may be specified by WAF installation and/or content container control information. This information may specify that certain areas and/or precise locations within properties should be used for fingerprinting, such as one or more certain fields of information or information types. Fingerprinting information may be incorporated into a property by modifying in a normally undetectable way color frequency and/or the brightness of certain image pixels, by slightly modifying certain audio signals as to frequency, by modifying font character formation, etc. Fingerprint information, itself, should be encrypted so as to make it particularly difficult for tampered fingerprints to be interpreted as valid. Variations in fingerprint locations for different copies of the same property; "false" fingerprint information; and multiple copies of fingerprint information within a specific property or other content which copies employ different fingerprinting techniques such as information distribution patterns, frequency and/or brightness manipulation, and encryption related techniques, are features of the present invention for increasing the difficulty of an unauthorized individual identifying fingerprint locations and erasing and/or modifying fingerprint information. provide smart object agents that can carry requests, data, and/or methods, including budgets, authorizations, credit or currency, and content. For example, smart objects may travel to and/or from remote information resource locations and fulfill requests for electronic information content. Smart objects can, for example, be transmitted to a remote location to perform a specified database search on behalf of a user or otherwise "intelligently" search remote one or more repositories of information for user desired information. After identifying desired information at one or more remote locations, by for example, performing one or more database searches, a smart object may return via communication to the user in the form of a secure "return object" containing retrieved information. A user may be charged for the remote retrieving of information, the returning of information to the user's WAF installation, and/or the use of such information. In the latter case, a user may be charged only for the information in the return object that the user actually uses. Smart objects may have the means to request use of one or more services and/or resources. Services include locating other services and/or resources such as information resources, language or format translation, processing, credit (or additional credit) authorization, etc. Resources include reference databases, networks, high powered or specialized computing resources (the smart object may carry information to another computer to be efficiently processed and then return

the information to the sending WAF installation), remote object repositories, etc. Smart objects can make efficient use of remote resources (e.g. centralized databases, super computers, etc.) while providing a secure means for charging users based on information and/or resources actually used. support both "translations" of WAF electronic agreements elements into modern language printed agreement elements (such as English language agreements) and translations of electronic rights protection/transaction management modern language agreement elements to electronic WAF agreement elements. This feature requires maintaining a library of textual language that corresponds to WAF load modules and/or methods and/or component assemblies. As WAF methods are proposed and/or employed for WAF agreements, a listing of textual terms and conditions can be produced by a WAF user application which, in a preferred embodiment, provides phrases, sentences and/or paragraphs that have been stored and correspond to said methods and/or assemblies. This feature preferably employs artificial intelligence capabilities to analyze and automatically determine, and/or assist one or more users to determine, the proper order and relationship between the library elements corresponding to the chosen methods and/or assemblies so as to compose some or all portions of a legal or descriptive document. One or more users, and/or preferably an attorney (if the document a legal, binding agreement), would review the generated document material upon completion and employ such additional textual information and/or editing as necessary to describe non electronic transaction elements of the agreement and make any other improvements that may be necessary. These features further support employing modern language tools that allow one or more users to make selections from choices and provide answers to questions and to produce a WAF electronic agreement from such a process. This process can be interactive and the WAF agreement formulation process may employ artificial intelligence expert system technology that learns from responses and, where appropriate and based at least in part on said responses, provides further choices and/or questions which "evolves" the desired WAF electronic agreement. support the use of multiple WAF secure subsystems in a single WAF installation. Various security and/or performance advantages may be realized by employing a distributed WAF design within a single WAF installation. For example, designing a hardware based WAF secure subsystem into an electronic appliance WAF display device, and designing said subsystem's integration with said display device so that it is as close as possible to the point of display, will increase the security for video materials by making it materially more difficult to "steal" decrypted video information as it moves from outside to inside the video system. Ideally, for example, a WAF secure hardware module would be in the same physical package as the actual display monitor, such as within the packaging of a video monitor or other display device, and such device would be designed, to the extent commercially practical, to be as tamper resistant as reasonable. As another example, embedding a WAF hardware module into an I/O peripheral may have certain advantages from the standpoint of overall system throughput. If multiple WAF instances are employed within the same WAF installation, these instances will ideally share resources to the extent practical, such as WAF instances storing certain control information and content and/or appliance usage information on the same mass storage device and in the same WAF management database. requiring reporting and payment compliance by employing exhaustion of budgets and time ageing of keys. For example, a WAF commercial arrangement and associated content control information may involve a content provider's content and the use of clearinghouse credit for payment for end-user usage of said content. Control information regarding said arrangement may be delivered to a user's (of said content) WAF installation and/or said financial clearinghouse's WAF installation. Said control information might require said clearinghouse to prepare and telecommunicate to said content provider both content usage based information in a certain form, and content usage payment in the form of electronic credit (such credit might be "owned" by the provider after receipt and used in lieu of the availability or adequacy of electronic currency) and/or electronic currency. This delivery of information and payment may employ trusted WAF installation secure subsystems to securely, and in some embodiments, automatically, provide in the manner specified by said control information, said

usage information and payment content. Features of the present invention help ensure that a requirement that a clearinghouse report such usage information and payment content will be observed. For example, if one participant to a WAF electronic agreement fails to observe such information reporting and/or paying obligation, another participant can stop the delinquent party from successfully participating in WAF activities related to such agreement. For example, if required usage information and payment was not reported as specified by content control information, the "injured" party can fail to provide, through failing to securely communicate from his WAF installation secure subsystem, one or more pieces of secure information necessary for the continuance of one or more critical processes. For example, failure to report information and/or payment from a clearinghouse to a content provider (as well as any security failures or other disturbing irregularities) can result in the content provider not providing key and/or budget refresh information to the clearinghouse, which information can be necessary to authorize use of the clearinghouse's credit for usage of the provider's content and which the clearinghouse would communicate to end-user's during a content usage reporting communication between the clearinghouse and end-user. As another example, a distributor that failed to make payments and/or report usage information to a content provider might find that their budget for creating permissions records to distribute the content provider's content to users, and/or a security budget limiting one or more other aspect of their use of the provider's content, are not being refreshed by the content provider, once exhausted or timed-out (for example, at a predetermined date). In these and other cases, the offended party might decide not to refresh time ageing keys that had "aged out." Such a use of time aged keys has a similar impact as failing to refresh budgets or time-aged authorizations. support smart card implementations of the present invention in the form of portable electronic appliances, including cards that can be employed as secure credit, banking, and/or money cards. A feature of the present invention is the use of portable WAFs as transaction cards at retail and other establishments, wherein such cards can "dock" with an establishment terminal that has a WAF secure sub-system and/or an online connection to a WAF secure and/or otherwise secure and compatible subsystem, such as a "trusted" financial clearinghouse (e.g., VISA, Mastercard). The WAF card and the terminal (and/or online connection) can securely exchange information related to a transaction, with credit and/or electronic currency being transferred to a merchant and/or clearinghouse and transaction information flowing back to the card. Such a card can be used for transaction activities of all sorts. A docking station, such as a PCMCIA connector on an electronic appliance, such as a personal computer, can receive a consumer's WAF card at home. Such a station/card combination can be used for on-line transactions in the same manner as a WAF installation that is permanently installed in such an electronic appliance. The card can be used as an "electronic wallet" and contain electronic currency as well as credit provided by a clearinghouse. The card can act as a convergence point for financial activities of a consumer regarding many, if not all, merchant, banking, and on-line financial transactions, including supporting home banking activities. A consumer can receive his paycheck and/or investment earnings and/or "authentic" WAF content container secured detailed information on such receipts, through on-line connections. A user can send digital currency to another party with a WAF arrangement, including giving away such currency. A WAF card can retain details of transactions in a highly secure and database organized fashion so that financially related information is both consolidated and very easily retrieved and/or analyzed. Because of the WAF security, including use of effective encryption, authentication, digital signaturing, and secure database structures, the records contained within a WAF card arrangement may be accepted as valid transaction records for government and/or corporate recordkeeping requirements. In some embodiments of the present invention a WAF card may employ docking station and/or electronic appliance storage means and/or share other WAF arrangement means local to said appliance and/or available across a network, to augment the information storage capacity of the WAF card, by for example, storing dated, and/or archived, backup information. Taxes relating to some or all of an individual's financial activities may be automatically computed based on "authentic" information securely stored and

available to said WAF card. Said information may be stored in said card, in said docking station, in an associated electronic appliance, and/or other device operatively attached thereto, and/or remotely, such as at a remote server site. A card's data, e.g. transaction history, can be backed up to an individual's personal computer or other electronic appliance and such an appliance may have an integrated WAF installation of its own. A current transaction, recent transactions (for redundancy), or all or other selected card data may be backed up to a remote backup repository, such a WAF compatible repository at a financial clearinghouse, during each or periodic docking for a financial transaction and/or information communication such as a user/merchant transaction. Backing up at least the current transaction during a connection with another party's WAF installation (for example a WAF installation that is also on a financial or general purpose electronic network), by posting transaction information to a remote clearinghouse and/or bank, can ensure that sufficient backup is conducted to enable complete reconstruction of WAF card internal information in the event of a card failure or loss. support certification processes that ensure authorized interoperability between various WAF installations so as to prevent WAF arrangements and/or installations that unacceptably deviate in specification protocols from other WAF arrangements and/or installations from interoperating in a manner that may introduce security (integrity and/or confidentiality of WAF secured information), process control, and/or software compatibility problems. Certification validates the identity of WAF installations and/or their components, as well as WAF users. Certification data can also serve as information that contributes to determining the decommissioning or other change related to WAF sites. support the separation of fundamental transaction control processes through the use of event (triggered) based method control mechanisms. These event methods trigger one or more other WAF methods (which are available to a secure WAF sub-system) and are used to carry out WAF managed transaction related processing. These triggered methods include independently (separably) and securely processable component billing management methods, budgeting management methods, metering management methods, and related auditing management processes. As a result of this feature of the present invention, independent triggering of metering, auditing, billing, and budgeting methods, the present invention is able to efficiently, concurrently support multiple financial currencies (e.g. dollars, marks, yen) and content related budgets, and/or billing increments as well as very flexible content distribution models. support, complete, modular separation of the control structures related to (1) content event triggering, (2) auditing, (3) budgeting (including specifying no right of use or unlimited right of use), (4) billing, and (5) user identity (WAF installation, client name, department, network, and/or user, etc.). The independence of these WAF control structures provides a flexible system which allows plural relationships between two or more of these structures, for example, the ability to associate a financial budget with different event trigger structures (that are put in place to enable controlling content based on its logical portions). Without such separation between these basic WAF capabilities, it would be more difficult to efficiently maintain separate metering, budgeting, identification, and/or billing activities which involve the same, differing (including overlapping), or entirely different, portions of content for metering, billing, budgeting, and user identification, for example, paying fees associated with usage of content, performing home banking, managing advertising services, etc. WAF modular separation of these basic capabilities supports the programming of plural, "arbitrary" relationships between one or differing content portions (and/or portion units) and budgeting, auditing, and/or billing control information. For example, under WAF, a budget limit of $200 dollars or 300 German Marks a month may be enforced for decryption of a certain database and 2 U.S. Dollars or 3 German Marks may be charged for each record of said database decrypted (depending on user selected currency). Such usage can be metered while an additional audit for user profile purposes can be prepared recording the identity of each filed displayed. Additionally, further metering can be conducted regarding the number of said database bytes that have been decrypted, and a related security budget may prevent the decrypting of more than 5% of the total bytes of said database per year. The

user may also, under WAF (if allowed by senior control information), collect audit information reflecting usage of database fields by different

Detailed Description Text (1349):
Since different users may wish to interact differently, there may be many right answers to the personalization strategy. Some users are self serving and want to have the tools to explore or make choices on their own, others want immediacy, others may want intimacy such that their feed back and options register with the company. See FIG. 100 for a graphical depiction of personalization from no customization at 10000 to one-on-one personalization at 10002.

Detailed Description Text (1395):
Explicit information capture usually provides an interface to collect profile information. The site explicitly asks the user to provide the information. Examples of explicit information capture techniques are: Registration Forms. A form that the user fills out to register to the site. This may include interests, demographics or any other profile attributes that site has defined and the user may be willing to provide. Static or Dynamic Questionnaires. During the interaction, the site may prompt the user to answer questions. The questions may be based on the answer to the previous question. (Note: The registration form or a rating interface may also be an example of a questionnaire.) The site might ask a user a question if there is a Personalization Knowledge Gap. (A Personalization Knowledge Gap is the difference between the data required to deliver a specific personalized interaction and the amount of information the site has collected on the user.) Another example might be a need assessment questionnaire. For example Progressive Insurance's site provides a list of questions used to analyze the user's insurance needs. Rating Interface. The site may provide an interface that allows the user to rate content or products. A rating interface is often used with collaborative filtering. Filter or Query Interface. An interface that allows the user to directly manipulate or filter the content that is displayed. Configuration Interface. An interface that allows the user to configure the site or select the content to be displayed.

Detailed Description Text (1585):
Security Technical Description Encryption services are provided in the security architecture of FIG. 116 with Virtual Private Networking (VPN). The central corporate firewall 11600 has a server VPN module 11602, and all remote customer locations are required to implement a VPN module on their firewall 11604 as well. Remote users 11606 will need client VPN software installed on their PCs. Remote users should also implement a local encrypting application that will encrypt the contents of sensitive directories on their hard drive. Authentication services are provided to users at customer locations with digital certificates. The central corporate headquarters will maintain a CA (Certificate Authority) to administer the certificates. The CA is integrated with an LDAP server to store directory information. An RA (Registration Authority) is used to process certificate requests. For users at customer locations, the authentication occurs at the corporate web server and is managed by the web server access control software. Stronger authentication is required for remote users because they have increased access in the internal network. Remote users therefore will be issued smart cards on which they will store their private key. Each remote user will need a smart card reader for their PC. Access control is provided by firewalls at entry points into both the corporate headquarters network and the customer location. A secondary firewall is located behind the web server at corporate headquarters to further restrict access to more sensitive servers on the internal network. An access control software package 11608 is used on the web servers to restrict access to specific web pages, files, and directories. In addition, all sensitive servers at corporate headquarters (database, ftp, application, firewall, web) have hardened operating systems implemented either with a specific secure server or an add on software package. Integrity is provided with digital fingerprint technology at the ftp server. As a user downloads a file to their PC, it is stamped with a digital fingerprint which uniquely identifies the time and the user that downloaded that

file. Auditing services are provided in real time with Intrusion Detection Modules (IDM) on all critical services. Off line auditing is provided with operating system security scanning tools to identify vulnerabilities.

Detailed Description Text (1595):
FIG. 119 illustrates an exemplary architecture. In this sample architecture, customers 11900 are provided with the capability to access account information, pay bills, order checks, and transfer funds between their multiple accounts. The customer will use a PC to dial their ISP 11902 and access the bank's web site. The client PC will be equipped with standard HTML browser software, and HTTP communications capability for connectivity to the server 11904 at the bank. An encrypted session is established between the client and the server using SSLv3. Once a connection is established, the customer can request a service from the bank's web site. This request consists of the recall of an ASP or HTML page, using a secure SSL3/PCT session over TCP/IP.

Detailed Description Text (1598):
Customer launches a web browser and goes to the bank's web site. The encryption server creates a secure SSL session and requests a login name and password. Authentication is passed to the application server and verified. The main page provides user with different options such as account information, funds transfer, bill payments, portfolio management and a loan service center. Customer wants to pay bills but first clicks on account information to check his balance. The web server requests the account information from the application server which accesses the mainframe for the data. Account information including balance, recent deposits and cleared checks are returned to the web server and displayed on the user's computer. User decides to pay bills and clicks on bill payment User enters the name of the payee and the application server queries the mainframe for the payee's address and information about previous checks written to this payee by the user. User enters an amount and the date it should be paid. Data is transferred to the application server and executed on the assigned date. Money is then transferred out of the user's account and cleared with the payee's bank through the banks clearing house. User logs out and the SSL session ends.

Detailed Description Text (1600):
Security Technical Description Encryption services are provided between the client 12000 and the server 12002 with SSLv3 using 128 bit session keys. The encrypted session is between the client PC and the encryption server 12004. Note that this requires clients to have browsers which support SSLv3. Authentication services are provided with digital certificates. Customers will be issued personal digital certificates 12006, signed by the root key for the bank. The encryption server will have a server side certificate signed by a leading PKI provider. Certificate management services will be outsourced, so that the bank will approve and deny certificate requests at the RA (Registration Authority), but certificate revocation and management services will be provided by a PKI service vendor 12008. Access control is provided by a firewall 12010 at the entry point into the bank's network. A packet filter router is placed in front of the firewall server, and a choke router is placed behind the firewall in order to provide some redundancy at this critical juncture. The firewall should implement Network Address Translation (NAT) to protect configuration information of the bank's internal network. Customer profiles which limit customer's access to the application and the mainframe are maintained on a database off of the application server. Users are given unique IDs and privileges to access the application and the mainframe. In addition all sensitive servers at the bank (firewall, encryption, application, web) have hardened operating systems implemented either with a specific secure server or an add on software package. Integrity is provided with digital signatures on the transaction messages sent from the client PC to the application server. Auditing services are provided in real time with Intrusion Detection Modules (IDM) on all critical services. Off line auditing is provided with operating system security scanning tools to identify vulnerabilities. In addition, a single transaction ID is

logged at each point in the architecture to provide the ability to trace a single transaction through multiple audit logs.

Detailed Description Text (1607):
Security Technical Description Encryption services are provided between the client 12200 and the web server 12202 at the storefront with SSLv3 using 128 bit session keys 12204. Note that this requires clients to have browsers which support SSLv3. To secure file transfer between the storefront and the merchants, a toolkit is used to implement encryption services at application server 12206 (storefront) and the fulfillment server 12208 (merchant). Authentication services are provided between the merchant and storefront with digital certificates, implemented with the same security toolkit as the encryption services. Certificate management will be performed by the storefront with a leading CA (Certificate Authority) product. An RA (Registration Authority) is used to process certificate requests. Customers will not be uniquely authenticated. The storefront web server will have a server side certificate signed by a leading CA provider to authenticate itself to customers. Access control is provided by a firewall at the entry point into the storefront network. A packet filter router is located before the web server to limit traffic to the web server to HTTP only. In addition all sensitive servers at the storefront (firewall, database, application, web) have hardened operating systems implemented either with a specific secure server or an add on software package. Integrity is provided on the file transfer between the merchant and storefront with digital signatures implemented at the application server and fulfillment server. Auditing services are provided in real time with Intrusion Detection Modules (IDM) on all critical services. Off line auditing is provided with operating system security scanning tools to identify vulnerabilities. Fraud Services are provided by a separate company that specializes in secure payment technologies. The storefront will collect order and payment information from the customers, and will pass this information to the payment/fraud services company to check the credit card numbers for fraud attempts, and to approve and process the transactions. An encryption toolkit is used between the application server and the payment services architecture to secure the transactions between the two networks.

Detailed Description Text (1756):
In another exemplary embodiment of the present invention, payment of the amount of money that the buyer owes the seller is requested, such as through sending the user a bill. Further, the amount of money for the reallocated bandwidth can be received from the seller, where it will be processed and sent to the seller, placed in an account of the seller, and/or used to pay amounts of money the seller owes to a third party or for the transaction fee.

Detailed Description Text (1757):
In an alternate embodiment, an operator captures consumer payment directives using a telephone with a small text display. These consumer payment directives are sent to a central computer operated by the system, which then uses an automated teller machine network to obtain funds in the amount of the payment from the consumer's automated teller machine-accessible bank account. Once the funds are obtained into an account of the system operator, the system determines how to pay the biller, either by wire transfer, debit network using the biller's bank account number, or by check and list.

Detailed Description Text (1758):
Several exemplary embodiments of the present invention for performing clearing and settlement functions include bill pay or remittance processing systems as set forth below. For brevity and clarity, the consumer's account with the biller is referred to herein as the C-B ("consumer-biller") account, thereby distinguishing that account from other accounts: the consumer's account with its bank, the biller's account with its bank, etc. In most cases, the biller uses the C-B account number to uniquely identify the consumer in its records.

Detailed Description Text (1759):
Bill pay transactions, however accomplished, have several common elements, which are either explicit or can be implied by the nature of the transaction. The first is presentment: a biller presents the consumer with a bill showing the C-B account number and an amount due. The second common element is payment authorization: the consumer performs some act (e.g., signs a check or other negotiable instrument) which authorizes the consumer's bank to transfer funds from the consumer's account to the biller; this element might occur after presentment or before (as in the case of pre-authorized withdrawals), and need not be explicit (delivery of a check is implicit authorization for the amount of the check). This element is almost always accompanied by some action by the consumer bank to ensure payment to it from the consumer, such as withdrawing the funds from consumer's bank account, posting the amount to the consumer's credit card account or line of credit, etc. The third common element is confirmation to the consumer of the funds withdrawal. The fourth common element is the crediting of the payment to the C-B account. In some cases, the biller acknowledges the crediting with nothing more than refraining from sending a past due bill.

Detailed Description Text (1760):
FIGS. 141 through 143 show block diagrams of bill pay systems which implement these four common elements in different ways. In those block diagrams, the participants are shown in ovals, and the flow of material is shown by numbered arrows roughly indicating the chronological order in which the flows normally occur. The arrows embody a link, which is a physical link for paper flow, a data communications channel from one point to another, or other means for transferring material. Where several alternatives exist for a flow, the alternatives might be shown with a common number and a letter appended thereto, such as "2" and "2A". "Material" refers to documents and/or information, whether paper-based ("postal mail"), electronic (e-mail, messages, packets, etc.), or other transfer medium. In most cases, the material which is flowing is shown near the arrow which links the material's source and destination.

Detailed Description Text (1761):
FIG. 141 is a block diagram of a paper bill pay system 14100, wherein billers send paper bills or coupon books to consumers and consumers return paper checks and payment coupons. The proof and capture process for these remittances is highly automated, except for the aptly-named "exception items."

Detailed Description Text (1762):
In bill pay system 14100, the participants are a consumer C (14102), a biller B (14104), consumer C's bank (Bank C) 14106, biller B's bank (Bank B) 14108 and, optionally, a lockbox operator 14110. Bank C maintains consumer C's bank account 14112 and a clearing account 14114, while Bank B maintains biller B's bank account 14116 and a clearing account 14118. The material passing between the participants includes a bill 14120, a remittance 14122 comprising a check 14124 and a payment coupon 14126, an account statement 14128, an accounts receivable ("A/R") data file 14130, an encoded check, which is check 14124 with MICR encoding, and possibly a non-sufficient funds ("NSF") notice 14136.

Detailed Description Text (1763):
The flow of material between participants in bill pay system 14100 begins (arrow 1) when biller B sends bill 14120 through the postal mails to consumer C. Bill 14120 indicates a C-B account number and an amount due, and is typically divided into an invoice portion to be retained by consumer C and a payment coupon portion to be returned, each of which shows the C-B account number and amount due.

Detailed Description Text (1764):
In response to receiving bill 14120, consumer C sends remittance 14122 to biller B (arrow 2). Remittance 14122 contains check 14124 drawn on consumer C's account 14112 at Bank C and payment coupon 14126, preferably included in the return

envelope provided by biller B. Biller B then MICR encodes the amount of the remittance onto check 14124 to create encoded check 14134, and deposits check 14134 (arrow 3), and credits consumer C's account in biller B's customer general ledger ("G/L") account database 14132. Alternately, remittance 14122 is mailed to lockbox operator 14110 (arrow 2A), which opens remittance 14122, MICR encodes check 14124 to create encoded check 14134, captures the C-B account number and amount of the check electronically to create A/R data file 14130. Lockbox operator 14110 then sends A/R data file 14130 to biller B, and sends encoded check 14134 to Bank B to be credited to biller B's account 14116 (arrow 3A). Because check 14134 is signed by consumer C, it authorizes Bank C to pass the amount of the check to Bank B after Bank B presents the check to Bank C. The signed check serves as the second common element of a bill pay transaction: authorization.

Detailed Description Text (1766):
If the funds are not available in C's account 14112 to cover the amount of check 14134 or if C's account 14112 has been closed, then Bank C will return the check to Bank B, who will in turn return the check to biller B. Biller B will then have to reverse the transaction crediting consumer C's C-B account in G/L database 14132 and renegotiate payment from consumer C, all at significant cost to biller B. Even if check 14134 clears, the process of providing good funds to biller B is not instantaneous, since check 14134 must physically travel from biller B to Bank B to Bank C. Of course, if biller B has sufficient credit rating with Bank B, Bank B could move the funds from clearing account 14118 to B's account 14116 when Bank B receives check 14134.

Detailed Description Text (1767):
At some time following the clearing of check 14134, biller B also updates its A/R records in G/L database 14132 to credit consumer C's C-B account, and Bank C confirms to consumer C the withdrawal of the amount of check 14134 by listing it on statement 14128 and/or by the return of cancelled check 14134. If the check doesn't clear, then biller B and other parties to the transaction unwind the payment.

Detailed Description Text (1768):
One benefit of bill pay system 14100 is that, for nearly all billers, there is no need for biller enrollment (any consumer can pay a biller without prior arrangements or a waiting period).

Detailed Description Text (1769):
Similar to the above system is the GIRO systems used in several countries in Northern Europe. The GIRO systems were set up there either by the government or the postal system, which is a traditional supplier of financial services. In a GIRO system, it is mandated that each bill payer and each bill payee be assigned a GIRO number. The biller sends bills with its biller GIRO number on the payment coupons. The layout, shape, etc. of the GIRO payment coupons is also mandated, so a consumer will receive similar coupons with each bill. After reviewing the bill, the consumer simply adds their GIRO number to the payment coupon and signs it. Thus, the payment coupon also serves as a banking instrument similar to a check.

Detailed Description Text (1770):
The consumers in a GIRO system are comfortable with it because the payment coupons all look the same. The consumer then mails the payment coupons to either a GIRO central processor or its own bank, which then sorts them by biller GIRO number and submits them to the biller. Since the payment coupons are all in a fixed format, they can be easily encoded in a machine readable format, including the payment amount, which the biller pre-prints onto the coupon. If the consumer gives their GIRO number to the biller, the biller can also pre-print that number on the payment coupon as well. Since all the coupons look the same, the banks can process them like a check and achieve economies of scale.

Detailed Description Text (1771):

FIG. 142 is a block diagram of an alternate bill pay system 14200, which reduces the effort required on the part of consumer C relative to bill pay system 14100, but which increases costs for billers. The difference between bill pay system 14200 and bill pay system 14100 is that consumer C initiates payment electronically (or by other non-check means).

Detailed Description Text (1772):
Bill pay system 14200 includes most of the same participants as bill pay system 14100: consumer C, Bank C, Bank B, possibly a lockbox operator (not shown in FIG. 142), and biller B, who is typically not a proactive or willing participant in this system. Additionally, a service bureau S (14202) and a Bank S (14204) are participants, with service bureau S maintaining a service database 14206 which is used to match bill payment orders with billers. The material passing among the participants includes bill 14120, as in the prior example, as well as a bill payment order 14208 and related confirmation of receipt 14216 (both typically transmitted electronically), an enrollment package 14209, a biller confirmation 14210, a bill payment 14212 ("check and list") which includes check 14214.

Detailed Description Text (1773):
In bill pay system 14200, consumer C enrolls in bill pay system 14200 by sending service bureau S (arrow 1) enrollment package 14209 comprising a voided check and list of billers to be paid by S on behalf of C. S subsequently sends biller B biller confirmation 14210 (arrow 2) to verify (arrow 3) that C is indeed a customer of B.

Detailed Description Text (1774):
With bill pay system 14100 (FIG. 141), consumer C identifies the proper biller by the remittance envelope and the payment coupon, neither of which is available to service bureau S in bill pay system 14200. Thus, service bureau S must identify the correct biller for each bill payment order some other way. Typically, service bureau S does this by asking consumer C for biller B's name, address, telephone number and consumer C's account number with biller B ("C-B account number"). Since neither Bank C nor service bureau S may have any account relationship with biller B, they must rely upon consumer C's accuracy in preparing enrollment package 14209 which is used to put biller B's information into service database 14206. Service bureau S typically requires this information only once, during biller enrollment, storing it to service database 14206 for use with subsequent payments directed to the same billers. Of course, if this information changes, service database 14206 would be out of date. If this information is wrong to start with, or becomes wrong after a change, service bureau S might send funds to the wrong entity. What a service bureau will often do to reduce errors in biller identification is to not allow the consumer to make payments to a biller for a specified time period after enrolling the biller, to allow service bureau S to verify biller B and the C-B account structure with biller B in a biller confirmation message 14210.

Detailed Description Text (1775):
Sometime later, consumer C receives bill 14120 (arrow 4) and initiates bill payment order 14208 (arrow 5). Bill payment order 14208 includes authorization for service bureau S to withdraw funds from C's account 14112 to pay bill 14120, the amount to pay (not necessarily the amount due on bill 14120), the date on which to pay, and some indication of biller B as the payee. Service bureau S responds with confirmation of receipt 14216 indicating that bill pay order 14208 was received (arrow 6). Consumer C can send bill pay order 14208 in any number of ways, such as using a personal computer and modem, directly or through a packet of other data network, via an automatic teller machine (ATM), video touch screen, a screen phone, or telephone Touch-Tone.TM. pad (TTP) interacting with a voice response unit (VRU). However this is done, service bureau S receives one or more bill pay orders from consumer C. These orders could be instructions to pay some amount for a bill or a set amount of money at periodic intervals.

Detailed Description Text (1776):
Assuming that service bureau S has correctly identified and confirmed that biller B is a biller which consumer C desired to pay with bill pay order 14208, then service bureau S passes the funds to biller B as biller payment 14212 (arrow 12) after securing funds to cover the remittance. Bill payment can take several forms as discussed below. In FIG. 142 a "check and list" is depicted, which is common in the art. A check and list comprises a single payment, check 14214 drawn on service bureau S's account 14218, accompanied by a list of all consumers whose individual remittances are aggregated in the single check. The list shows C-B account numbers and payment amounts for each consumer included on the list which should total to the amount of the single check 14214. This process brings some economies of scale to service bureau S, although at additional expense to biller B. In some cases, rather than endure the expense of checking over the list to ensure it matches the check amount, biller B will refuse to accept that form of payment.

Detailed Description Text (1777):
To secure funds, service bureau S clears check 14134 through Bank S 14204 drawn on C's account 14112 at Bank C (arrows 7-11). S then sends payment 14212 to biller B (arrow 12). Biller B must treat payment 14212 as an exception item, posting G/L database 14132 from the list instead of payment coupons as in bill pay system 14100. Biller B deposits check 14214 with Bank B (arrow 13) who clears it through Bank S and a settlement account 14220 to obtain good funds for B's account 14116 (arrows 14-142). If the bill pay transaction goes through, Bank C will confirm that it went through by sending a confirmation (typically statement 14128) to consumer C. The cycle is completed (arrow 18) when consumer C receives notice that funds were withdrawn from C's account 14112 for the amount entered in bill pay order 14208.

Detailed Description Text (1778):
Several variations of the system shown in FIG. 142 are used today. In one variation, S sends an individual check 14134 (unsigned--signature on file) drawn on C's account 14112 to biller B in response to bill pay order 14208. This clears as in bill pay system 14100 (FIG. 141, arrows 3-7), but B must process these one at a time, since they are exception items. This reduces the possibility that B will refuse to process check 14134, since it only differs from the expected payment form by lacking a coupon. Thus, biller B is less likely to refuse this form of payment over a check and list, and the biller is less likely to have problems of the list not balancing or having bad account numbers.

Detailed Description Text (1780):
FIG. 143 is a block diagram of yet another bill pay system 14300, which is usually used with billers who expect regular, periodic and small payments. Relative to the previously discussed bill payment systems, billers generally prefer bill pay system 14300 when they are set up to handle such transactions.

Detailed Description Text (1781):
Bill pay system 14300, while providing more efficient remittance processing by biller B due to its increased control over the process, leaves consumer C with very little control over the bill pay transactions after the relationship is set up, since consumer C is typically required to give biller B an open ended authorization to withdraw funds. Furthermore, bill pay system 14300 is not appropriate for all types of billers, such as those who do not have an on-going and predictable relationship with consumers.

Detailed Description Text (1782):
FIG. 143 introduces several new items which flow among the participants including ACH 14302, such as a voided check 14306, a debit advice 14308, a pre-authorization message 14310, and a debit request message 14312. In bill pay system 14300, biller B is required to maintain an additional customer database 14304.

Detailed Description Text (1783):
For bill pay system 14300 to work properly, there is an enrollment phase (arrows 1-4) and an operational phase (arrows 5-13). In the enrollment phase, consumer C gives biller B voided check 14306, which biller B uses to initiate pre-authorization message 14310. Biller B is not allowed by ACH 14302 to directly submit pre-authorization message 14310, which means Bank B, an ACH Originating Financial Depository Institution (OFDI), must get involved and submit message 14310 to Bank C, an ACH Receiving Financial Depository Institution (RFDI). After pre-authorization message 14310 is accepted by Bank C, Bank C will accept Bank B initiated automatic debits to be posted to C's account 14112. In the operational phase, biller B queries customer database 14304 to determine if consumer C is enrolled as an automatic debitor. If so, biller B optionally sends debit advice 14308 to consumer C, and sends debit request message 14312 to biller B's bank, Bank B, which then sends it through the ACH 14302 to Bank C, which debits C's account 14112 and transfers the funds to biller B's account 14116 via the ACH. The transaction is confirmed to consumer C on bank statement 14128 sent to consumer C from Bank C. In this system 14300, debit request message 14312 might be rejected by Bank C for, among other reasons, non-sufficient funds, resulting in the flows along arrows 10-12.

Previous Doc Next Doc Go to Doc#